②

人間－ロボット系の安全性評価に関する研究

平成２年８月

佐藤吉信

目　　次

ページ

第1章　緒　　論

1．1　研究の背景

産業用ロボットが、危険・有害作業を作業者に代替して行うという産業安全上望ましい機能をもつ反面、ロボット自体が労働災害の原因となりうることについては、いくつかのロボットによる災害事例からも明らかである[1, 2]。また、将来、産業用ロボットに限らず、知能移動ロボットなどの開発によって、保全作業、緊急時の救援作業、あるいは我々の日常生活にもロボットの普及が考えられる[3, 4]。このような状況に至った場合、その安全性が社会的にも重要な関心事となるであろうことは想像に難くない。

特に産業用ロボットに関しては、その潜在的な危険性に対処するために、労働安全衛生規則が一部改正されるとともに、その使用に関する技術指針なども公示されている[5]。また、ISO/TC184/SC2/WG3 により作られた「産業用マニピュレーティング・ロボット－安全性」国際規格（原案）は、産業用ロボットに対する安全性の要求事項とガイドラインを示している[6]。これらにより、その時点での産業用ロボットに対する安全上の指針が示されたことになる。

この国際規格（原案）と、従来のクレーンや工作機械などの産業用機械に対する安全規格との比較において著しい特徴は、ロボットの設計段階または使用段階で個々の系ごとに安全解析を実施し、その安全性を事前に評価することが要求されている点にある。これは、産業用ロボットが、そのタイプ、使用方法および他の設備や機械との関係によって動作パターンが異なってくるなどのため危険の性質が多様であること、ロボット自体の技術革新が非常に著しいスピードで行われ常に新しい問題が生じ得ること、硬直的な規制は技術進歩を阻害する恐れがあること、などの理由により生じたものである。

安全工学の観点からみたとき、ロボットと従来の機械・装置との最大の相違

点は、ロボットの融通性にある。高度なロボットほど、その用途も多岐にわたり、製造者の予想をこえた目的に使用される可能性がある[7]。また、介護ロボット、外科用ロボットなどでは積極的に人間と接触することがその本来の機能目的となろう[8, 9, 10]。

このように、ロボットは、従来の機械に比し安全化の戦略がいっそう複雑となるため、系統的な安全設計を実施して、事前に安全性を確保しておく必要がある。また、その安全性の達成レベルを査定し、そのレベルが許容できるかを評価しておかなければならない。従って、ロボットの安全性を事前に評価するための方法論の確立が緊急の課題となっている。

本論文は、人間－ロボット系の事前安全性評価の問題をシステムズ・アプローチの観点から取扱うものである。

1．2　研究の位置付け

系の安全化を計る一連の活動すなわち安全計画は、すでに発生した災害の再発を防止するための事後安全計画と、潜在的に発生の可能性のある災害を事前に予防する事前安全計画とに大別できる。

系統的な安全計画の実施手順は、図１－１のようになろう。すなわち、事前安全計画では、先ずデータ収集に基づいて系に生ずる潜在危険が同定され、以下順次、潜在危険抑制手段の概念化、そのような抑制手段を採用した条件下での定性的安全解析、・・・などが行われる。一方、事後安全計画では、災害原因の調査に基づき同類の災害の抑制手段が検討され、以下同様に、系の定性的安全解析、定量的安全解析、・・・などが順次行われる。

このような系の安全計画において、安全性評価に課せられる範囲は、主として手順1、2、3、4 である。従って、安全性評価においても、すでに十分に運用経験があり災害統計なども得られる系に対して行うことのできる事後安全性評価と、新しい系や災害経験の乏しい系を対象として行う事前安全性評価とに大別できる。事後安全性評価では、例えば、度数率や強度率などの労働災害統計量

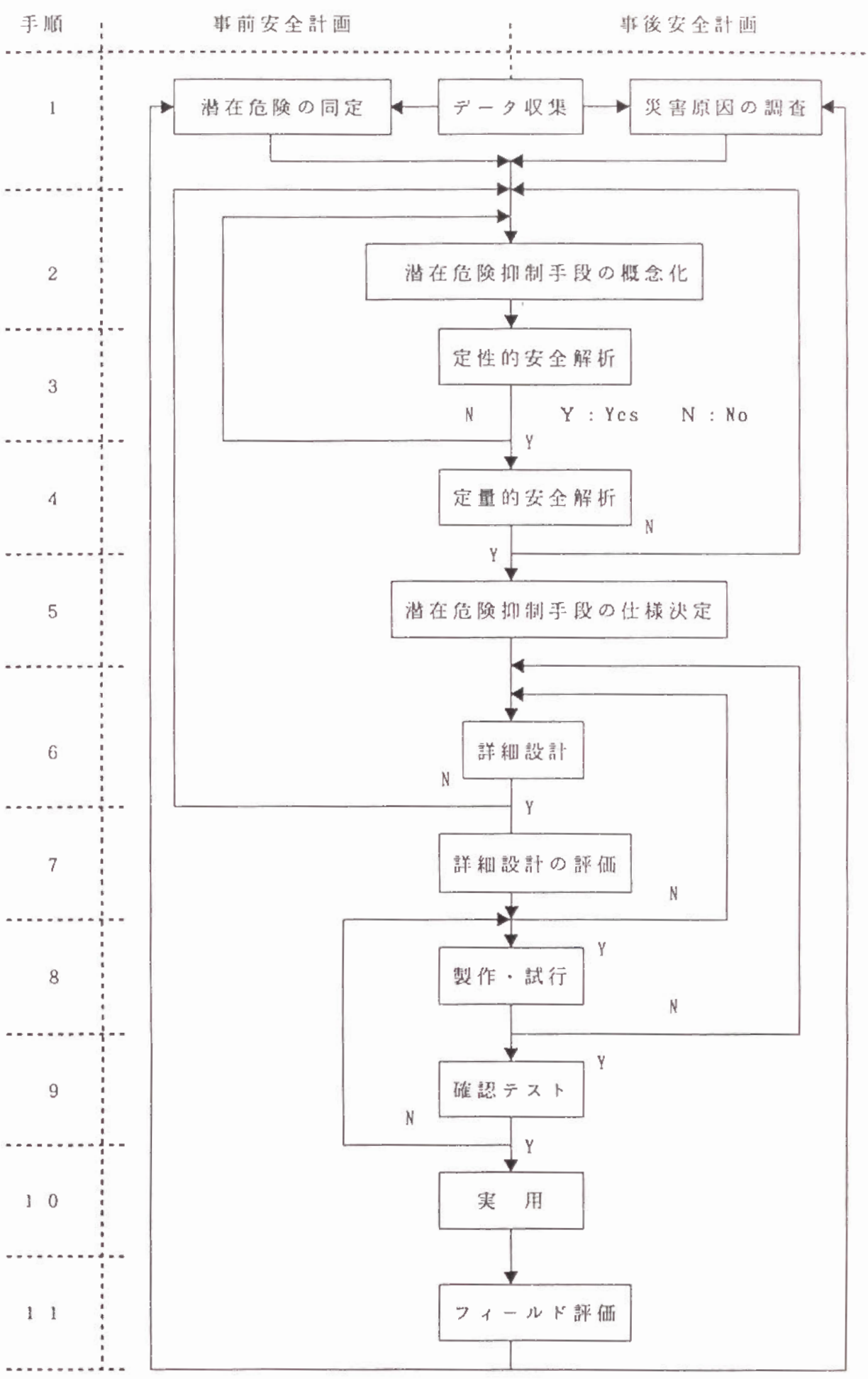


図1-1 安全計画の実施手順

から系の安全性を評価でき、花安は建設工事労働災害を統計学的に分析することにより建設工事全般の安全性評価を行っている[11]。事前安全性評価に関する報告としては、原子力施設の安全性評価を行ったWASH-1400 が代表的なものとしてあげられる[12]。

ロボットなどから構成される新しい系の事前安全性評価は、安全計画手順1, 2, 3, 4 から構成される次の系統的手順によって行われる必要がある[13, 14]：

（1）潜在危険の同定
（2）潜在危険抑制措置の検討
（3）定性的安全性解析
（4）定量的安全性解析

ここで、潜在危険の同定とは、系内にどのような故障や異常が発生して、その結果どのような毀損が発生しうるかを帰納的に予測し見極める作業を意味する。次に、同定された潜在危険に対して、どのような抑制措置を採用できるかを検討し、その抑制措置の条件下で系の安全性を評価するために定性的安全性解析、さらに定量的安全性解析を実施しなければならない。これにより、選択可能な抑制措置から最善のものを採用することができる。また、安全性解析の結果によっては、手順(2) に戻って再び潜在危険抑制措置を再構成しなければならないこともある。安全性解析によって、潜在危険抑制措置構築のための詳細設計条件が与えられる。

特にロボットなどを用いた柔軟で多機能な系では、安全計画上の見落しを防ぐため各手順が系統的な方法論に基づいて行われる必要がある。

ここで、ロボットの安全性に関する分野でのこれまでの研究成果を概説し、本論文の位置付けを明確にする。

杉本[15]、土橋[16]、Preis [17]、Muldau[18]、Inaba [19]、Carlsson[20]、Nicolaisen [21]、川口[22, 23]などにより、すでに産業用ロボットの潜在危険性が認識され、災害事例や個々の技術対応策が論じ始められた[24~29]。

長町らは、人間工学的見地から産業用ロボット操作時の人間の信頼性および産業用ロボットの安全対策に対するコスト－効果問題について論じている[30]。Khodabandehlooらは、油圧サーボ駆動制御ロボットのポンプ、バルブ、アクチュエータなどの要素に対して故障要因分析を行った[31]。Rahimiは人間－産業用ロボット系の防護装置に対してエネルギ障壁解析を行い[32]、Goossensは過去の産業用ロボット災害事例から８種類の典型的な事故シナリオを抽出するとともに、教示作業時の残存リスクを確率論的に推定している[33]。この他、産業用ロボットの安全性について、事故データ、災害事例、信頼性データ、そして個々の具体的な安全対策についての研究が多数報告されている[34-49]。

以上の報告は、災害事例とその防止のための個々の技術的対応策に関する研究がほとんどであり、これらの研究には安全技術の体系化や系統的な事前安全性評価に関するものは含まれていない。

今後出現の予想される知能移動ロボットなど新しいロボットの安全性が確保されるためには、設計段階や使用計画段階での事前安全性評価が上述の手順に従い、系統的方法論に基づいて行われなければならない。

本論文では、今後出現の予想されるロボットも含めて、人間－ロボット系の事前安全性評価を行うための系統的方法論について論ずる。以降、安全性評価を事前安全性評価の意味で用いる。

本論文の内容と構成は次の通りである。

第２章では、人間－ロボット系に生ずる潜在危険を同定するための系統的方法論について論ずる。まず、毀損発生過程を、系の要素間での作用の授受とそれによる要素の変化としてモデル化し、作用および変化を分類・体系化する。次に、潜在危険の同定を行うための「作用－変化と作用連鎖モデル」を提案する。これにより、潜在危険の概念を明確化するとともに、人間－ロボット系で生ずる潜在危険を包括的に同定する。

第３章では、まず、潜在危険の抑制過程を、作用－変化と作用連鎖モデルに基づいて、４段階に体系化し、その最終的な抑制過程は、潜在危険制御系が発現しつつある潜在危険を毀損の発生する前に解消する過程であることを示す。次に、潜在危険制御系の構成法則を、作用鎖の解離原理として体系化する。これにより、潜在危険の同定と有機的に結びついた、潜在危険制御系構成のための系統的な方法論を確立する。さらに、フェイル・セーフやフォールト・トレラント・システムなどの概念を明確化し、それら安全技術の潜在危険制御系への適用法則を明らかにする。そして、自律移動ロボットの潜在危険制御系を基本構成し、その情報処理系へのフェイル・セーフやフォールト・トレラント・システムの適用性をあきらかにする。

第４章では、同定された潜在危険による災害の発生機構を演繹的に解析するための包括的論理モデルを構成する。これにより、個々の系に実施された定性的解析に見落しがないかをチェックすることができる。また、具体的な系の災害発生論理は、本章で構成される論理モデルの部分集合として与えることが可能となる。論理モデルの構成は定量的評価への欠くことのできない過程であり、定量的評価に必要な条件を考察し、系の相分割を論ずる。

第５章では、人間－ロボット系における安全性の定量的評価のための方法論について論ずる。人間－ロボット系では、災害の発生が系の要素の故障発生順序に依存するため、順序依存形故障論理の定量化が必要であることを述べ、その定量化のためのアルゴリズムについて論ずる。

第６章では、ＦＡ機械工場における産業用ロボットなどから構成される無人加工セルを取りあげ、５章までに論じた方法論に基づいて安全性評価を行う。これにより、実際の安全性評価において、これまでに論じてきた方法論がどのように相互に関連づけられ適用されるかを示す。また、それら方法論の有効性を検証する。

本論文は、参考文献1, 7, 50～65, 92, 97, 98 に基づいて纏めたものである。

第２章　潜在危険の同定

２．１　緒　　言

原子力プラント、化学プラント、航空機など従来の系は、複雑であるが、ロボットのように多目的に使用されることはない。これらの系を対象として、その信頼性および安全性を解析するための方法論としてFMEA(Failure Mode and Effect Analysis), ETA(Event Tree Analysis), FTA(Fault Tree Analysis) などが研究され、今日では広く一般に使用されている[66]。このうち、ETA と FTA は、系の定性的あるいは定量的解析すなわち安全性評価手順(3) および (4) を実施するためのものである[67]。

FMEAは、装置の安全上重要な箇所など特定の部分に対して、部品やサブシステムの故障頻度やその影響を評価するための手法である。しかし、装置のハードウエアの故障を主な検討対象としているため、ヒューマン・エラーなどによる操作の失敗などは考慮されない。また、一連の故障伝播の最初のひき金となる異常または故障にどのようなものを考えるべきか、故障の影響の伝播形態としてどのようなものを考えるべきかについて体系的な方法論を与えていない。

一方、HAZOP(Hazard and Operability Study)[68] は、プラントにおける潜在危険の同定のために開発された手法である。これは、プラントの各プロセスおよび各要素において、その正常稼働状態からの考え得る可能な逸脱状態を表に示すことを行い、それらの逸脱がどのようにして生ずるのかを検討し、それがプラントにどのような影響を与えるかを予測するための手法である。この予測に基づき、それらの逸脱状態を検出し、処理するための手段が吟味される。

HAZOP は、逸脱状態発掘のためのガイド・ワードが、流量、圧力、温度、水位などプラントに密接した物理量に限定的な "None", "More of", "Less of", "Part of", "More than", "Other" などであるため、人間－ロボット系への

適用は困難である[69]。

ロボットは、構造系、駆動系、制御系、センサ系などハード体系、および人工知能を実現するためのソフト体系など工学全般にわたる体系から構成される。ロボット自体が複雑な系であり、その柔軟な機能性により多様な環境で多目的に使用されるようになる。このため、ロボットと環境との干渉によって、多様な危険性が生ずることが予測され、安全性評価の第1段階「潜在危険の同定」過程が、他の系の場合に比して特に重要である。しかしながら、上述のように、これまで人間－ロボット系に生ずる潜在危険を系統的に同定するための方法論が研究されていない。

本章では、毀損発生過程を、系の要素間での作用の授受による変化と作用連鎖の生成過程としてモデル化し、複雑で柔軟な系に生ずる潜在危険を系統的に同定するための方法論を展開する。これに基づき、人間－ロボット系に生じ得る潜在危険を包括的に同定する。

2.2 作用－変化と作用連鎖モデル

潜在危険（Hazard）の概念についての公認された定義はない。一般には、例えば「ある情況において、エラー、見落とし、変化そしてストレスの連鎖が、物または人身の損害を伴うエネルギの望ましくない移行（Transfer）に結びつく潜在力」という定義[70]とほぼ同様の概念として用いられる場合が多い。文献(71)なども、この概念の延長としてのエネルギ伝播モデルによって潜在危険を論じている。

それらの定義は、何らかのエネルギが要素間で移行する結果、災害が生ずるという災害発生論の観点を反映したものと思われるが、機能が果たされないことや、情報や病原体あるいは心理的影響によっても生ずる災害をすべて網羅するには不完全である。また、潜在危険生成過程に置ける系の要素間の関係が適切に体系化されていない。そこで、毀損の生成過程を以下のようにモデル化し、要素間の関係を分類・体系化することにより、潜在危険を系統的に同定可能と

する方法論を展開する。

２．２．１　要素間における作用と変化

一般に、系が、人間、構造物、機械装置、物質、環境条件、遂行目標などの各要素から構成されているとき、ある要素に毀損が生ずる過程に、他の要素の介在が含まれる場合と含まれない場合とがある。毀損を生ずる要素が人間であるなら、後者の場合は災害とは言えない。したがって、本論文では、要素と要素の関係によって毀損を生ずる場合のみを考えるものとする。

系のある要素の毀損発生過程における要素間の関係は、要素から要素への作用の授受とそれによって生ずる要素の動作や状態における変化（故障、異常、エラーも含む）の過程として把握することができる。作用の連鎖がいくつかの要素間で成立することにより、ある要素の毀損発生の必要条件となる作用が生起する。図２－１はこのような作用連鎖の要素ＸとＷの部分を示したもので、要素Ｘの変化が（ｘ）で、要素ＸからＷへの作用が矢印で、さらにこれが引金となって要素Ｗに生ずる変化が（ｗ）で表されている。

要素間での作用を調べると、次のようなａからｆまでの６種類に分類することができ、各形の作用を定義することにより作用の全体的概念が明確化される。

［定義２－１］

ａ．エネルギ伝播形作用：運動エネルギや熱エネルギなど、エネルギとしての意味をもつ要素間での働きかけとする。エネルギの授受により要素には、エネルギ変換による変化が生じ得る。

ｂ．情報伝達形作用：表示や信号など、情報としての意味をもつ働きかけとする。情報の授受により、制御系などの状態に変化が生じ得る。

ｃ．作因物転移形作用：化学物質や病原体あるいは重量物などのように、エネルギや情報以外の物質として認識できる作因物が要素から要素へと授受されることによる働きかけとする。作因物の授受により、化学変化、ポテンシャル・エネルギや濃度の変化、質量の変化などが生ずる。

ｄ．供給阻害形作用：ある要素に、エネルギ、情報または作因物などの必需が

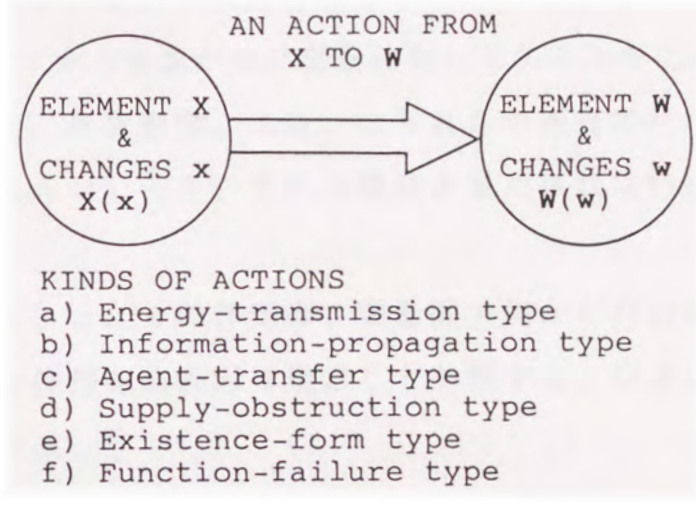


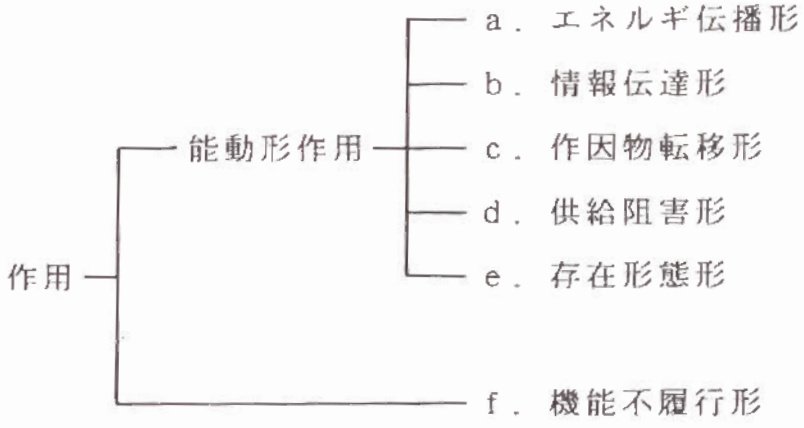
図2-1 要素間の作用・変化モデル

あって、それに対する供給を妨害することによる働きかけとする。供給阻害作用により、例えば人間なら窒息、装置ならば運転停止などの変化が生ずる。

e．存在形態形作用：エネルギ、情報および作因物の移動を伴わなず、それらの供給を妨害するものでもない、要素間でのある要素の形状、重量、状態、条件などによるａ、ｂ、ｃ、ｄ、ｆ以外の働きかけとする。

f．機能不履行形作用：ある要素が他の要素に対してエネルギ伝播、情報伝達、作因物転移、供給阻止、存在形態、あるいはそれらの複合された働きすなわち機能を行わなければならないとき、それら機能が果たされないことによる作用とする。

ここで、ａ、ｂ、ｃ、ｄ、ｅの作用は、要素間で何かが行われることにより生ずるので、これらの作用を能動形作用として分類する。以上により、作用は次のように体系化される：



２．２．２　作用連鎖

ここでは、ある要素ＡからＢへの作用には、他の要素の媒介がなく行われるものとする。仮に、要素Ｃの媒介があれば、要素ＡからＣへの作用と、要素ＣからＢへの作用が行われたものと考える。作用には、例えばある種の運動エネルギのように、２要素の接触によって伝播が行われるものと、音のエネルギが空気によって伝播される場合のように２要素間の媒体によって伝えられるもの、および光のエネルギのように放射によって伝播されるものとがある。接触による場合には、他の要素の媒介がないことは明らかであるが、他の場合において

も、作用を伝える媒体が、その作用の性質や強度を望ましくない方向に変化させないかぎりにおいては、その媒体を系の要素とはしないこととし、したがって、その場合には2要素間の作用として考えるものとする。

［定義２－２］系のある要素に作用して、その要素にある毀損を生じさせる必要条件となる作用を、その要素のある毀損発生に関する直接原因作用と言う。

［定義２－３］ある要素ＡからＢへの作用が、要素Ｂからのある作用の発生確率を増大させるとき、この要素ＡからＢへの作用を、その要素Ｂからの作用の誘因作用と言う。

ある要素にある毀損が生ずるための必要条件となる直接原因作用の発現過程は、系の要素間で、いくつかの誘因作用が次々と連鎖してその直接原因作用に結びつく、方向性のある一連の作用連鎖として把握される。さらに、系のある要素ＡからＢへの作用連鎖は、要素Ａ、Ｂ、および他の要素との関係において、以下のようないくつかの形に分類される。

［定義２－４］

作用連鎖１形：要素ＡからＢへの直接原因作用が行われるもの。

作用連鎖２形：要素ＡからＢへ直接原因作用は行われないが、誘因作用が行われ、Ａ以外の要素からＢへ直接原因作用が行われるもの。

作用連鎖３形：要素ＡからＢへの直接原因や誘因作用は行われないが、要素Ｂへ直接原因作用を行う要素Ｃに対して、要素Ａからの誘因作用があるもの。

作用連鎖４形：要素ＡからＢへの直接原因作用、誘因作用および要素Ｂへ直接原因作用を行う要素への誘因作用が行われない作用連鎖とする。

作用連鎖の各形における連鎖例を図２－２に示す。図中、要素間の作用の授受を矢印で表し、矢印の下の数字が零のときは、その作用が直接原因作用であり、矢印の下の数字が、ｉ（≧１）のときは、その作用がｉ－１の作用の誘因作用であることを表している。任意の作用連鎖は各形におけるいくつかの作用連鎖を合成することによって得られる。例えば、図２－２の中の複合連鎖例は、連鎖順序が３→２→１→０の２形と、２＊→１＊→０の３形が合成されたものとなっている。なお、特別な場合として、毀損発生の必要条件に関する知見が

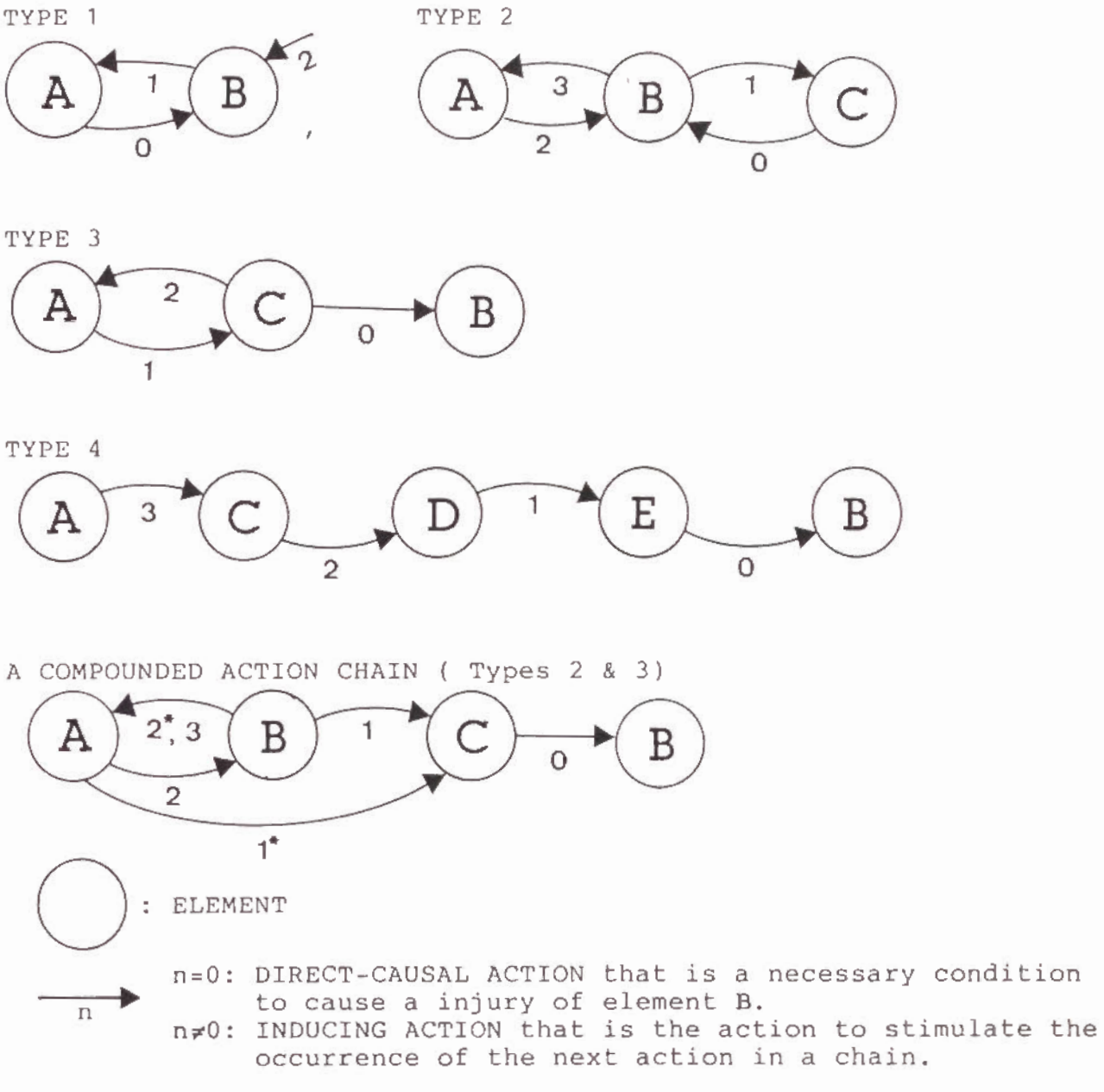


図2-2 各連鎖形における作用連鎖例

不明などによる、直接原因作用のない作用連鎖２形と４形が、図２－２の２形と４形の連鎖例において、それぞれ要素ＢとＣ、要素ＢとＥを同一要素とすることにより得られる。

２．２．３　潜在危険の定義

毀損の生成過程を、前述の６種類の作用が要素間で連鎖・伝播していく過程としてモデル化して表す方法を「作用－変化と作用連鎖モデル」（以下単に、Ａ－Ｃモデル）と言うこととする。Ａ－Ｃモデルに基づいて、潜在危険を以下のように定義する。

［定義２－５］系のある要素Ａが要素Ｂに、ある毀損発生への直接原因を行う潜在力を、その系における、その毀損発生に関する要素Ａの要素Ｂに対する直接潜在危険と定義する。

［定義２－６］要素Ａが、要素Ｂのある毀損発生の直接原因作用は行わないものの、その作用連鎖の中の誘因作用を行う潜在力を、同様に間接潜在危険と定義する。

［定義２－７］要素Ａの要素Ｂに対する直接潜在危険と間接潜在危険の全集合を、その系における要素ＡのＢに対する全潜在危険と定義する。

したがって、要素ＡのＢに対する潜在危険の同定とは、その系で生じ得る各要素の作用と変化、それによって生ずる要素ＡからＢへの作用連鎖、そして要素Ｂに生ずる毀損の性質を、可能なかぎり同定することである。

２．３　ロボットの潜在危険

２．３．１　ロボットへの作用と変化

ロボットへの作用とそれによる変化は以下のように同定される。

ａ）エネルギ伝播形作用

接触により伝播し得るものとして、運動エネルギ、熱エネルギ、そして電気的エネルギが、媒体により伝播し得るものには爆風などの運動エネルギ、音響

的振動エネルギ、熱流などによる熱エネルギ、体中を伝播する電気エネルギが、そして放射によるものとして、可視光線、赤外線、紫外線、レーザー光線、アーク、電子ビーム、X線、電磁波そして放射線などがある。

これらの作用により、ロボットの転倒、機械的破損、部材の劣化、制御系の故障、制御系への異常信号の発生、制御の不能、誤動作などの変化が生じる。

b）情報伝播形作用

他要素との整合性を保持するために必要な情報伝達経路などから、ロボットに誤信号が伝達されると、運動状態、運動量などに変化が生じ得る。

c）作因物転移形作用

腐食性物質や、放射性物質などの作用により、電子回路やセンサの損傷、機械的部分の破損や劣化、制御系への異常信号の発生などが生じる。

d）供給阻害形作用

ロボットに必需されるものとして、動力源の供給、情報などがあるとき、これらの供給が阻害されると、制御の不能や誤動作が生じ得る。

e）存在形態形作用

重力の作用、ロボットの移動経路の状態などの環境条件により、ロボットの運動状態の変化、制御変量の逸脱が生じる。

f）機能不履行形作用

ロボットへの情報やエネルギ供給機能が働かないと、ロボットに制御不能や誤作動などの変化が生じる。

2．3．2　人間への作用と変化・毀損

a）エネルギ伝播形作用

人体に作用するエネルギには、接触により伝播される運動エネルギ、熱エネルギそして電気的エネルギ、媒体によって伝播される運動エネルギ、音響・振動エネルギ、熱流などの熱エネルギそして海水中を電導する電気的エネルギなど、さらに放射により伝播される赤外線、紫外線、レーザ光、アーク、電子ビーム，X線、電磁波そして放射線などいわゆる放射エネルギおよびそれらの複合

されたものが考えられる。これらの作用は、人体に対して直接原因作用としても、誘因作用としても働き得る。

直接原因作用として働くと、運動エネルギでは、打たれ、切られ、押しつぶされることによる、骨折、関接傷害、内臓損傷、創傷、表皮損傷、打撲傷、そして破砕傷などが生ずる。熱エネルギでは、火傷、凍傷、熱射病などが、電気的エネルギでは、感電によるショックや火傷が、音響振動エネルギでは聴力障害や振動障害が、いわゆる放射エネルギでは、火傷、視力障害、感電によるショック、X線障害そして放射線障害などが生じ得る。

誘因作用として働いた場合には、生理的反応または心理的動揺による各種の誤動作やヒューマン・エラーを誘発させ得る。

b）情報伝達形作用

主として誘因作用として働き、判断に影響を与えることにより、各種のヒューマン・エラーを誘発させ得る。

特別な場合として、心因性障害の直接原因作用としても働き得る。

c）作因物転移形作用

作因物としては、一酸化炭素などの中毒性物質、高・低温物質、酸・アルカリ性の腐敗性物質、有機溶剤などの化学物質そして細菌やビールスなどの病原体などが考えられる。

これらが直接原因作用として働くと、中毒、火傷、凍傷、表皮損傷、粘膜または内臓損傷、視力障害、呼吸困難による窒息そして細菌やビールスによる疾病などが生じ得る。

誘因作用として働くと各種のヒューマン・エラーを誘発させ得る。

d）供給阻害形作用

人間に必需される供給には、呼吸気としての空気（酸素）、ある状況においては、情報、飲食物そして体温保持のためのエネルギなどが考えられる。

これらの供給阻害作用が、直接原因として働くと、窒息、失調症、などが生じ得る。

誘因作用として働くと、熱射病や各種のヒューマン・エラーを誘発させ得る。

e）存在形態形作用

人間に作用する存在形態としては、人間に対するその要素の位置的関係、形状、重量、また作業の難易性、職務の要求度そして各種の環境条件などが考えられる。これらの作用は、人間の位置エネルギ、運動エネルギ、生理的または心理的ストレスを増大させ得る。主として誘因作用として働き、ヒューマン・エラーの誘発や災害の形を規定する。職務の過度な要求度が精神障害の直接原因として働くなどの場合も生じ得る。

f）機能不履行形作用

人間に関係する機能には、呼吸気や情報などの供給機能、支持機構のような人間の存在条件を規定する補助機能、保護具や安全装置などの防護機能などが考えられる。

これらの機能の不履行が直接原因作用として働くと、例えば人工呼吸器の故障による窒息などが生じ得る。

誘因作用として働くと、墜落災害や、補助機能・防護機能が達成されないために生ずる各種の毀損、そしてヒューマン・エラーなどを誘発させ得る。

2．3．3　ロボットの作用とそれによる毀損

系の要素としてのロボットを、その本体、支援装置およびそれが所持している工具、加工物、材料などの扱い物も含めたものとして定義し、ロボットの行い得る作用とそれによる要素の変化そして毀損の形を同定する。

a）ロボットのエネルギ伝播形作用

［運動エネルギ］ロボットはその本体や所持物の自律的運動を行うほか、重力の作用や衝突あるいは把持物の放出などによる制御を逸した他律的運動も含めて運動エネルギによる作用を行い得る。

この直接原因作用により 2.3.2節で検討した各種の毀損が人体に生ずる。

作用連鎖２形での典型として、人間がロボットに押されることによる墜落・転倒・水中へ落下などの災害、危険域に入り込んだり、誤操作を行うなどにより他の要素からの各種の直接原因作用を受けることが考えられ、それによるさ

まざまな災害が生じ得る。

作用連鎖３形では、ロボットが周辺の装置に干渉したり、構造物を破壊するなどの誘因作用を行うなどによって、装置の誤動作や構造物の倒壊による直接原因作用が生じ得る。

［熱エネルギ］ロボット本体に高温部の存在するもの、高温物質、低温媒体、溶接工具などを扱うものでは、熱的エネルギによる作用が生じ得る。これによる直接原因作用により、2.3.2節で検討した各種の災害が生じ、作用連鎖２形と３形では、運動エネルギの場合と同様に、各種の災害を生じ得る。

［電気的エネルギ］ロボットは、その本体や工具などの電力源を有する場合に、これによる作用を行い得る。

この直接原因作用により、2.3.2節で検討した災害が生じ、作用連鎖２形や３形では、運動エネルギの場合と同様に各種の災害を生じ得る。

［振動エネルギ］ロボットの工具や本体から、騒音や振動が発生せられる場合には、この直接原因作用により、2.3.2節で検討した災害が生じ得る。誘因作用として働くと、心的ストレスや他装置への干渉により、ヒューマン・エラーや装置の誤動作を誘発する。

［放射エネルギ］ロボットの工具、センサおよび扱い物などが、いわゆる放射エネルギを発生する場合には、この直接原因作用により、2.3.2節で検討した各種の災害が生じ得る。作用連鎖２形、３形においては、ヒューマン・エラーや装置の誤動作などを誘発させる誘因作用として働く。

ｂ）ロボットの情報伝達形作用

他要素との整合を保持しなければならないロボットでは、信号などによる他要素との情報交換を行わなければならない。

作用連鎖２形では、人間が誤情報を受け取ることにより危険域に入って、他の要素の作用により災害が生ずることが考えられる。

作用連鎖３形では、ロボットからの情報による周辺の装置の動作によって、直接原因作用が人間に行われ、各種の災害が生ずる。

ｃ）ロボットの作因物転移形作用

中毒性物質、腐食性物質、放射性物質など有害物質を扱うロボットでは、それによる直接原因作用により、 2.3.2節で検討した各種の毀損を生じ得る。

作用連鎖２形、３形では、ヒューマン・エラーや装置の誤動作に結びつく誘因作用を行い、各種の災害が発生する。

ｄ）ロボットの供給阻害形作用

移動を行うなど高度なロボットほど、他の要素への干渉による供給阻害作用が生じやすくなることが考えられる。

作用連鎖３形で、エネルギや情報の供給阻害を受けた要素の誤動作や機能不履行による直接原因作用が人間に働き得、これにより各種の災害発生が考えられる。

ｅ）ロボットの存在形態形作用

ロボットによる存在形態形作用には、その形状、構造、位置的関係によるもの。また保全作業や設置作業そして教示作業などの難易度などがあり、ヒューマン・エラーや位置エネルギの増大による墜落災害などの誘因作用、さらに静止しているロボットに人間が打ち当たることによる反作用として働き得る。

ｆ）ロボットの機能不履行形作用

ロボットが人間の補助機能を行っているときには作用連鎖２形として、他の要素との連携機能を有するときには作用連鎖３形として誘因作用を働き得る。これによる各種災害が生じることが考えられる。

２．３．４　ロボットからの作用連鎖

実際に発生した産業用ロボットによる災害事例には次のようなものがある：作業者が、シェービング・マシンと、それに加工物を供給し取り出すための産業用ロボットからなる加工セルで、シェービング・マシンの調整を行っていた。作業終了後、マシンの起動ボタンを押したところ、シェービング・マシンからロボットへの作動命令が伝達されたためマニプレータが作業者の背後から伸展した。作業者は逃げる間もなく、マニプレータとシェービング・マシンとの間に身体を挟まれ死亡した。

この災害を作用連鎖モデルで記述すると図２－３となる。図中、記号Ｈ、Ｒ、Ｓ、(h)、(r)、(s)、･･･ により、それぞれ系の要素「作業者」、「ロボット」、「シェービング・マシン」および各要素の変化を表す。また、ａ、ｂ、ｃなどのアルファベットとアークおよびアーク下部の数字により、作用の授受とその作用の直接原因作用からの連鎖順位を示す。

すなわち、シェービング・マシンＳの調整完了[S(s)e $\xrightarrow{3}$] が作業者ＨのマシンＳの起動動作[H(h)b $\xrightarrow{2}$] を誘発させ、マシンＳからロボットＲへの作動命令が生じた[S(s')b $\xrightarrow{1}$]。さらに、マシンＳが存在していたため[S(s")e $\xrightarrow{2}$] 、作業者が逃げられずマニプレータの作動点に存在することとなり[H(h')e $\xrightarrow{1}$] 、直接原因作用が生じた[R(r)a $\xrightarrow{0}$]。

以上のことから明きらかのように、この災害は、

$$S(s)e \xrightarrow{3} H(h)b \xrightarrow{2} S(s')b \xrightarrow{1} R(r)a \xrightarrow{0} H(\cdot) \qquad (2\text{-}1)$$

$$S(s")e \xrightarrow{2} H(h')e \xrightarrow{1} R(r)a \xrightarrow{0} H(\cdot) \qquad (2\text{-}1)'$$

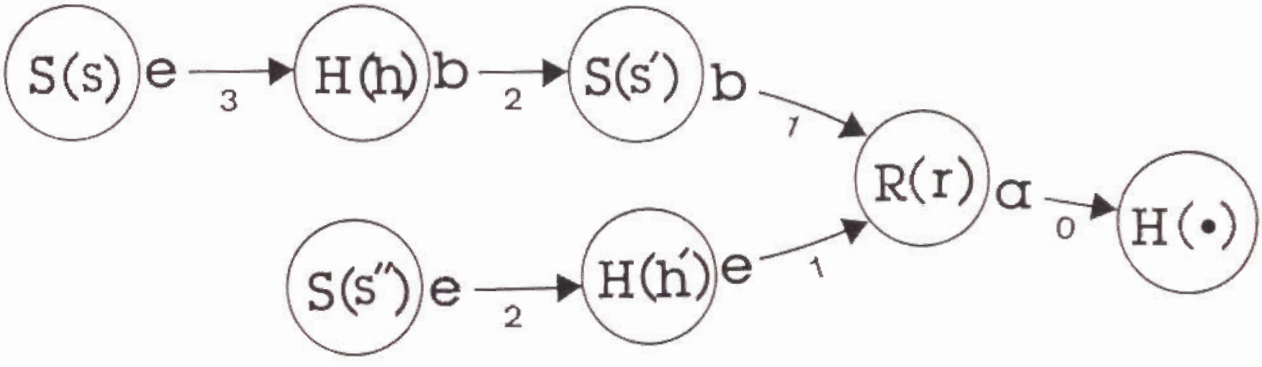
の少なくとも２通りの単連鎖からなる複合連鎖により構成されている。

このように、現実の災害は、何らかの複合連鎖の生起によって発生する場合が多い。しかし、本事例では、２つの作用連鎖を共に予見しなくとも、例えば作用連鎖(2-1) のみが予見できればその潜在危険を認識できる。従って、複合連鎖によって生ずる災害の発生も、その発生の主要な作用連鎖がひとつ同定されることによって予見可能となる。

更に厳密な災害発生理論の展開は、安全性評価の第３段階である災害発生機構の演繹的解析によって得られる。

表２－１には、ロボットから人間への典型的な作用連鎖（単連鎖）が同定されている。

各作用連鎖に対して、多様な具体的シナリオが考えられる。そのうち代表的なものについて、表２－２に示す。



H(h), H(h'): Human & Changes,　R(r): Robot & Changes

S(s), S(s'), S(s"): Shaving Machine & Changes,　H(・): Human & Injury

図2-3 実災害のＡ－Ｃモデル記述

表２－１　ロボットから人間への作用連鎖の同定（その１）

ロボットの作用	要素間の典型的作用連鎖
a）エネルギー伝播形	作用連鎖１形：R（a）$\xrightarrow[0]{a}$ H（・） H（h）$\xrightarrow[1]{a}$ R（r）$\xrightarrow[0]{a}$ H（・） H（h）$\xrightarrow[1]{e}$ R（r）$\xrightarrow[0]{a}$ H（・） R（r）$\xrightarrow[2]{e}$ H（h）$\xrightarrow[1]{a}$ R（r）$\xrightarrow[0]{a}$ H（・） H（h）$\xrightarrow[1]{b}$ R（r）$\xrightarrow[0]{a}$ H（・） ２：R（r）$\xrightarrow[2]{a}$ H（h）$\xrightarrow[1]{a}$ P（p）$\xrightarrow[0]{a}$ H（・） R（r）$\xrightarrow[2]{a}$ H（h）$\xrightarrow[1]{b}$ P（p）$\xrightarrow[0]{a}$ H（・） R（r）$\xrightarrow[2]{a}$ H（h）$\xrightarrow[1]{b}$ P（p）$\xrightarrow[0]{c}$ H（・） R（r）$\xrightarrow[2]{a}$ H（h）$\xrightarrow[1]{b}$ P（p）$\xrightarrow[0]{d}$ H（・） R（r）$\xrightarrow[2]{a}$ H（h）$\xrightarrow[1]{e}$ P（p）$\xrightarrow[0]{a}$ H（・） R（r）$\xrightarrow[2]{a}$ H（h）$\xrightarrow[1]{e}$ P（p）$\xrightarrow[0]{c}$ H（・） R（r）$\xrightarrow[2]{a}$ H（h）$\xrightarrow[1]{e}$ P（p）$\xrightarrow[0]{d}$ H（・） ３：R（r）$\xrightarrow[1]{a}$ P（p）$\xrightarrow[0]{a}$ H（・） R（r）$\xrightarrow[1]{a}$ P（p）$\xrightarrow[0]{e}$ H（・） R（r）$\xrightarrow[1]{a}$ P（p）$\xrightarrow[0]{d}$ H（・） R（r）$\xrightarrow[1]{a}$ P（p）$\xrightarrow[0]{f}$ H（・）

表２－１　ロボットから人間への作用連鎖の同定（その２）

b）情報伝達形	2：　R（r）$b \xrightarrow[2]{}$ H（h）$e \xrightarrow[1]{}$ P（p）$a \xrightarrow[0]{}$ H（・） 3：　R（r）$b \xrightarrow[1]{}$ P（p）$a \xrightarrow[0]{}$ H（・）
c）作因物転移形	1：　R（h）$c \xrightarrow[0]{}$ H（・） H（h）$a \xrightarrow[1]{}$ R（r）$c \xrightarrow[0]{}$ H（・） H（h）$b \xrightarrow[1]{}$ R（r）$c \xrightarrow[0]{}$ H（・） H（h）$e \xrightarrow[1]{}$ R（r）$c \xrightarrow[0]{}$ H（・） 2：　R（r）$c \xrightarrow[2]{}$ H（h）$a \xrightarrow[1]{}$ P（p）$a \xrightarrow[0]{}$ H（・） 3：　R（r）$c \xrightarrow[1]{}$ P（p）$a \xrightarrow[0]{}$ H（・） R（r）$c \xrightarrow[1]{}$ P（p）$c \xrightarrow[0]{}$ H（・） R（r）$c \xrightarrow[1]{}$ P（p）$d \xrightarrow[0]{}$ H（・） R（r）$c \xrightarrow[1]{}$ P（p）$f \xrightarrow[0]{}$ H（・）
d）供給阻害形	3：　R（r）$d \xrightarrow[1]{}$ P（p）$a \xrightarrow[0]{}$ H（・） R（r）$d \xrightarrow[1]{}$ P（p）$c \xrightarrow[0]{}$ H（・） R（r）$d \xrightarrow[1]{}$ P（p）$f \xrightarrow[0]{}$ H（・） 4：　R（r）$d \xrightarrow[2]{}$ P（p）$f \xrightarrow[1]{}$ Q（q）$a \xrightarrow[0]{}$ H（・）
e）存在形態形	1：　R（r）$e \xrightarrow[0]{}$ H（h） 2：　R（r）$e \xrightarrow[2]{}$ H（h）$a \xrightarrow[1]{}$ P（p）$a \xrightarrow[0]{}$ H（・） R（r）$e \xrightarrow[2]{}$ H（h）$b \xrightarrow[1]{}$ P（p）$c \xrightarrow[0]{}$ H（・）

表２－１　ロボットから人間への作用連鎖の同定（その３）

f）機能不履行形	1：　R（r）f $\xrightarrow[0]{}$ H（h）
	2：　R（r）f $\xrightarrow[2]{}$ H（h）a $\xrightarrow[1]{}$ P（p）a $\xrightarrow[0]{}$ H（・）
	R（r）f $\xrightarrow[2]{}$ H（h）e $\xrightarrow[1]{}$ P（p）c $\xrightarrow[0]{}$ H（・）
	3：　R（r）f $\xrightarrow[1]{}$ P（p）a $\xrightarrow[0]{}$ H（・）
	R（r）f $\xrightarrow[1]{}$ P（p）c $\xrightarrow[0]{}$ H（・）
	R（r）f $\xrightarrow[1]{}$ P（p）f $\xrightarrow[0]{}$ H（・）

表２－２　作用連鎖に想定される典型的シナリオ（その１）

作用連鎖	毀損発生のシナリオ例
$He \xrightarrow{1} Ra \xrightarrow{0} H(\cdot)$	人がロボットに近づいたとき、突然ロボットが人を打つ。
$Hb \xrightarrow{1} Ra \xrightarrow{0} H(\cdot)$	人が誤ってロボットを起動させて打たれる。
$Re \xrightarrow{1} Ha \xrightarrow{0} H(\cdot)$	人が停止しているロボットに打ちあたる。
$Ra \xrightarrow{3} He \xrightarrow{2} Pe \xrightarrow{1} Ha \xrightarrow{0} H(\cdot)$	人がロボットに押され、よろめいて構造物に打ちあたる。
$Ra \xrightarrow{2} He \xrightarrow{1} Pd \xrightarrow{0} H(\cdot)$	人がロボットに押され、水中に転落して溺れる。
$Ra \xrightarrow{2} Hb \xrightarrow{1} Pc \xrightarrow{0} H(\cdot)$	作業者がロボットに感電したはずみで装置のセンサに触れたため、装置から作業者に酸が降り注ぐ。
$Ra \xrightarrow{1} Pa \xrightarrow{0} H(\cdot)$	ロボットから電磁ノイズが発生し、装置が誤動作をして作業者を押し潰す。
$Ra \xrightarrow{1} Pc \xrightarrow{0} H(\cdot)$	ロボットが危険物保存容器を壊し、危険物が作業者に降り注ぐ。
$Ra \xrightarrow{1} Pf \xrightarrow{0} H(\cdot)$	ロボットが人工心肺を壊し、患者が窒息する。
$Rb \xrightarrow{2} He \xrightarrow{1} Pa \xrightarrow{0} H(\cdot)$	作業者がロボットからの誤情報によって危険域に入り、装置に押し潰される。
$Rb \xrightarrow{1} Pa \xrightarrow{0} H(\cdot)$	ロボットが装置のセンサに触れ、装置が起動して作業者が押し潰される。
$Ha \xrightarrow{1} Rc \xrightarrow{0} H(\cdot)$	作業者がロボットを揺動させたため、ロボットの把持していた危険・有害物質が作業者に降り注ぐ。

表２－２　作用連鎖に想定される典型的シナリオ（その２）

$Rc \xrightarrow[1]{} Pa \xrightarrow[0]{} H(\cdot)$	ロボットが導電物質を装置に降り注いだため、装置の電子回路が短絡して誤動作が発生し、作業者が装置に押し潰される。
$Rd \xrightarrow[1]{} Pf \xrightarrow[0]{} H(\cdot)$	ロボットが人工心肺の動力源を切断したため、患者が窒息する。
$Re \xrightarrow[3]{} He \xrightarrow[2]{} Pe \xrightarrow[1]{} Ha \xrightarrow[0]{} H(\cdot)$	ロボットが近づいてきたので、人があわてて逃げようとして構造物に打ちあたる。
$Rf \xrightarrow[0]{} H(\cdot)$	ロボットが乗員の呼吸用空気の供給に失敗し、乗員が窒息する。
$Rf \xrightarrow[3]{} He \xrightarrow[2]{} Pe \xrightarrow[1]{} Ha \xrightarrow[0]{} H(\cdot)$	ロボットが作業者の高所作業の支持に失敗し、作業者が墜落して地面に激突する。
$Rf \xrightarrow[1]{} Pa \xrightarrow[0]{} H(\cdot)$	ロボットが装置の運転に失敗し、装置が逆転して作業者を押し潰す。
$Rf \xrightarrow[1]{} Pc \xrightarrow[0]{} H(\cdot)$	ロボットが装置の操作に失敗し、装置から放射性物質が作業者に降り注ぐ。

ここでは、主として作用連鎖１、２、３形が検討されているが、４形はさらに他の要素が関係する２形と３形の延長されたものとなる。

表においては、記号R(r) によってロボットとその変化が、H(h) によって人間とその変化が、H(･) によって人間とその毀損発生が、P(p) 、Q(q) によって周辺要素とその変化が表されている。

２．４　潜在危険の集合論的表示

系の潜在危険集合を次のように定義する：

［定義２－８］系において、潜在危険を単連鎖からなる作用連鎖で同定したとき、それらの作用を発生させるその作用連鎖中の全変化、および直接原因作用から最も離れた作用を発生させる変化を直接または間接的に誘発させる系の全変化からなる集合を、その作用連鎖が同定する潜在危険集合とする。

定義より、系の全潜在危険集合は系の全変化集合として定義され、これを集合Hで表すものとする。

ここで、例えば次の２本の作用連鎖（単連鎖）：

$$X\ (x)\ a \xrightarrow{}_{0} W\ (\cdot) \qquad (2\text{-}2)$$

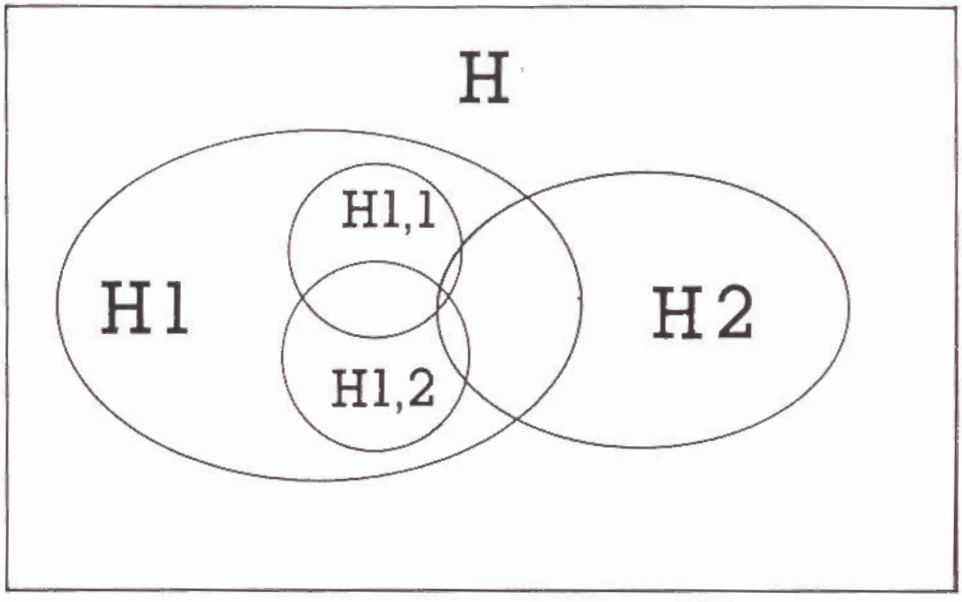
$$X\ (y)\ f \xrightarrow{}_{0} W\ (\cdot) \qquad (2\text{-}3)$$

が同定する潜在危険集合を、それぞれH1、H2とする。

すると、H1は作用鎖（$a \xrightarrow{}_{0}$）を発生させる要素X中の全変化集合x、および要素Xに結合して変化 x_i （$\in x$）を誘発させる全作用連鎖中の全変化集合からなる変化集合として定義される。H2も同様である。

さらに、次の作用連鎖：

$$A\ (a)\ a \xrightarrow{}_{1} X\ (x)\ a \xrightarrow{}_{0} W\ (\cdot) \qquad (2\text{-}4)$$



H　：全潜在危険集合

H1　：潜在危険集合［X（x）a $\xrightarrow{0}$ W（・）］

H2　：潜在危険集合［X（y）f $\xrightarrow{0}$ W（・）］

H1,1：潜在危険集合［A（a）a $\xrightarrow{1}$ X（x）a $\xrightarrow{0}$ W（・）］

H1,2：潜在危険集合［B（b）f $\xrightarrow{1}$ X（x）a $\xrightarrow{0}$ W（・）］

図2-4 潜在危険の集合論的表示

$$B(b)\ f \xrightarrow{1} X(x)\ a \xrightarrow{0} W(\cdot) \qquad (2\text{-}5)$$

で同定される潜在危険集合を、それぞれH1.1、H1.2と定義すると、系の全潜在危険集合H、部分潜在危険集合H1、H2、H1.1、H1.2との関係は、図２－４のように表される。

Hが枠内の全空間を占め、部分潜在危険集合がそれぞれの楕円および円内の領域を占める。領域の重なり合う部分は、それ等の作用連鎖が共に誘発される変化集合領域を示している。

２．５　結　言

本章では、人間－ロボット系の安全性評価の第１段階として、ロボットの潜在危険を同定した。

まず、毀損生成過程における系の要素間の関係を、作用－変化と作用連鎖モデルで体系化した。これにより、系内に生ずる潜在危険の概念およびその生成過程が明確化され、潜在危険が系統的に同定できるようになった。

次に、作用－変化と作用連鎖モデルを適用して、ロボットによって生じ得る作用、作用連鎖そして各要素の変化などを検討することにより、ロボットの人間に対する潜在危険が同定された。

系の条件が具体的に与えられることにより、作用連鎖２、３、４形における潜在危険もさらに詳細な同定が可能となる。

現在までのところ、ロボットによる災害はエネルギ伝播形作用による作用連鎖１形のものがほとんどであるが、今後、ロボットが高度化し、多方面に使用されるに従って、本章で同定された各種の潜在危険が問題となってこよう。

作用－変化と作用連鎖モデルによる系統的な同定結果は、安全性評価の後続の各段階と有機的に結びつくことにより、安全性評価全体に望ましい影響を与えることが期待できる。

第３章　潜在危険制御系の構成

３．１　緒　　言

マイクロ・コンピュータの発展は、単に工場における生産システムの変革のみならず、自動車などの交通手段や家庭用コンシューマ機器にいたるまで、種々の機械系のいわゆるメカトロニクス化の進展を促している。こうした系の安全性向上のためには、多様な潜在危険抑制措置が求められる。例えば、非常に厳格な安全性を要求されると言われる鉄道の電子連動装置では、いわゆる狭義のフェイル・セーフ技術(11%)、多重化などのいわゆる高信頼性技術(34%)、故障診断・回復(36%)、フール・プルーフ(4%)、危険側故障の低減(9%)、その他の技術(6%)など非常に多彩な潜在危険抑制措置によりその安全化がはかられていることがわかる[72]。

特にロボットは、構造系、駆動系、制御系、センサ系などのハード体系および人工知能を実現するためのソフト体系など工学全般にわたる体系から構成されそれ自体複雑な系であり、ロボットを含む系では、前章でみてきたように多様な潜在危険が生成される。このため、このような系に対しては、潜在危険抑制措置が系統的に検討される必要がある。

しかしながら、前章で述べたように、従来の安全性解析のための系統的方法論であるFMEA, ETA, FTA, HAZOPなどの方法論はいずれも安全性評価手順(1)、(3)、または(4)を対象としたものである。これまで、潜在危険抑制措置の検討は、個々の工学体系のエキスパートにまかされており[73]、異なる工学体系間に共通して適用可能となるよう体系化された潜在危険抑制措置構成のための系統的方法論が確立されていない。

たとえば、潜在危険抑制手段のひとつとしてフェイル・セーフ技術があるが、これは元来鉄道信号の分野で用いられ、信号系統に発生した障害が列車を停止

させる方向に収束するように系を構成する技術である。近年では、”フェイル・セーフ”の用語は、原子力プラントや航空機の設計などの広範な分野で用いられ、例えば航空機ではある種の冗長系を構成することをフェイル・セーフ技術と呼んでいるように、その意味するところが各分野で異なっている[74]。このような基本的術語をめぐる概念の不整合は、特に複雑な系の安全論議に混乱をもたらしている。

そこで本章では、A－Cモデルに基づき、まず 3.2節で潜在危険抑制措置を4段階の潜在危険抑制原理に体系化する。次に、 3.3節では、A－Cモデルを拡張して、系の最終的な潜在危険抑制過程を、潜在危険制御系による作用鎖の解離法則として一般化し、異なる工学体系間に共通した潜在危険制御系の構成のための系統的方法論を確立する。また、これに基づき、フェイル・セーフ・システムなどの概念を明確にし、その適用法則を明らかにする。さらに、 3.4節では、本方法論により移動ロボットの潜在危険制御系を構成し、その情報処理系へのフェイル・セーフ・システムの構成の可否を明らかにする。

3．2　潜在危険の抑制原理

A－Cモデルから、災害の防止は潜在危険の抑制すなわち作用連鎖の生成と発現を抑制することに他ならないという公理が導かれる。例えば、2.3.4 節で引用した実災害を防止する潜在危険抑制措置について考察してみよう：

（1）この系では、系の要素S，RまたはHが系の中に存在しなければ、作用連鎖［$S(s)e \xrightarrow{3} H(h)b \xrightarrow{2} S(s')b \xrightarrow{1} R(r)a \xrightarrow{0} H(\cdot)$］は生じないことは明らかである。

（2）それらの要素が存在しても、例えば変化(h) が抑制されれば作用連鎖の発現も抑制される。

（3）変化(h) が生じても、これに対するロボットの動作インターロッキング機構により、ロボットを作動させないようにしておけば直接原因作用鎖［$R(r)\ a \xrightarrow{0} H(\cdot)$］の発現は抑止される。

（４）さらに、作動中のロボットを非常停止させることによって、かろうじて災害の発生を阻止することが可能である。

以上の事例から明らかなように、潜在危険の抑制過程は、次の潜在危険抑制原理として分類・体系化される：

（１）作用源の排除

（２）変化の抑制

（３）系の毀損生成相遷移の禁止

（４）系の毀損生成相からの遷移

潜在危険抑制過程（１）は、人間または機器に望ましくない作用を行う要素を系から排除、またはそのエネルギー状態や化学的性質などを作用源とならない状態に限定して使用することを意味する。これは、排除する要素に代替する要素の存在、リスク、代替あるいは限定使用によるコスト増、社会的要請との関係など系の基本的設計条件により実現が決定される。

（２）は、要素が機能を維持し、危険側への逸脱した挙動を行わないようにすることである。余裕をもった条件による系の設計・運用、品質管理、高信頼性要素の採用、保全による信頼性の維持、教育・訓練によるヒューマン・エラーの防止、フール・プルーフなどによる危険側への変化の防止などによって達成される。

（３）において、系の相とは、系の要素の状態モードによって定まる系の相を意味する。例えば、ロボットの状態を停止モードと作動モードに区分すると、系を停止モード相と作動モード相とに分割することができる。今、系が停止モード相にあるとき、ロボットの制動系が正常でない、またはそのまま作動モード相へ遷移すると故障が生ずることが診断または予測できれば、系の停止モード相から作動モード相への遷移を禁止することができる。これは、異常診断、異常予測などによって達成される。

（４）は、系がすでに毀損の発生する相にあるとき、系の要素を制御することにより、毀損が回避される方向に系の状態を遷移させることを意味する。

潜在危険抑制原理(3)、(4) は、系に、ある条件下で発現しつつある作用連鎖

をその途中で解離することによって人間または重要な機器への毀損を回避する機構すなわち潜在危険制御系を構成することによって実現される。

３．３　潜在危険制御系の構成法則

３．３．１　作用鎖の解離

第２章で導入したＡ－Ｃモデルを以下のように拡張することにより、潜在危険制御系の基本的構成法則を明らかにする。

［定義３－１］系の要素は、分割された系の部分である。

［定義３－２］要素の変化は、電圧、温度などの物理量や形状、情報量の変化も含む。

｛性質３－１｝要素の毀損は作用によって生ずる。

｛性質３－２｝毀損の発現過程は、要素間での；１）作用の授受、２）要素の変化、でモデル化される。

［定義３－３］作用を行う要素を作用要素、作用を被る要素を被作用要素と言う。

［定義３－４］作用は定義２－１として定義される。

｛性質３－３｝作用は、ａ，ｂ，ｃ，ｄ，ｅ，ｆの各形に分類される。

｛性質３－４｝要素は、さらに下位要素に細分割される場合がある。

｛性質３－５｝作用は、要素間、および下位要素と上位要素間でも行われる。

［定義３－５］要素は、ａ，ｂ，ｃ，ｄ，ｅ　形の作用を行うとき、その作用に関して能動的な状態にある。

［定義３－６］能動的な状態にある要素を、その作用に関して作用源と言う。

［定義３－７］作用が行われる要素間の空間を、作用経路と言う。

［定義３－８］作用を発現させる特定の変化が生じている条件下で、作用連鎖のなかのある作用の発現を抑止することを、その作用鎖の解離と言う。

｛性質３－６｝誘因作用鎖が解離されると、次の作用の発生確率が減少し、直接原因作用鎖が解離されると、毀損の発生が抑止される。

［定義３－９］解離作用は、ある要素に作用して、その要素からの作用鎖を解離するための必要条件となる作用である。

［定義３－１０］解離作用を生成する要素を、解離要素と言う。

［定義３－１１］作用源の制御による作用鎖の解離を、作用源の制御と言う。

［定義３－１２］作用経路の制御による作用鎖の解離を、作用経路の制御と言う。

［定義３－１３］作用源と作用経路の制御による解離を、作用源と作用経路の制御と言う。

［定義３－１４］解離要素が機能不履行を行う要素の機能を代替することにより作用鎖を解離するとき、これを不履行機能の代替制御と言う。

｛性質３－７｝作用鎖の解離は、次の解離原理に分類される：

P_1．作用源の制御

P_2．作用経路の制御

P_3．作用源と作用経路の制御

P_4．不履行機能の代替制御

解離原理と作用鎖の解離との関係は、次の潜在危険制御系構成則として得られる：

［構成則３－１］能動（ａ，ｂ，ｃ，ｄ，ｅ）形の作用鎖は、解離原理P_1，P_2，P_3のいずれかにより、ｆ形の作用鎖は解離原理P_4によってのみ解離される。

［定義３－１５］解離作用を次のように分類する：

ａ’．エネルギ伝播形：解離要素と作用要素間でエネルギの授受が行われることにより生ずる解離作用。

ｂ’．情報伝達形：表示や信号など、存在形態やエネルギ量としてよりは情報量として意味をもつ働きがおこなわれることにより生ずる解離作用。

ｃ’．作因物転移形：化学物質、重量物など物質として認識可能な作因物の授

受により生ずる解離作用。

d'．供給阻止形：要素が作用を行うために、エネルギ、情報、作因物などの供給を必要とするとき、その供給を阻止することにより生ずる解離作用。

e'．存在形態形：エネルギ、情報、作因物の移動を伴わず、それらの供給を妨害するものでもない、形状、重量、状態、条件または性質などにより生ずるf'およびg' & g"以外の解離作用。

f'．機能停止形：解離要素が内部秩序状態にあることによって、解離要素と作用要素間で生じていた作用または複合された作用すなわち機能が停止することによって生ずる解離作用。

g' & g"．機能代替形：f形の作用を行うとしている要素に代わって、解離要素がその機能を代替することにより生ずる解離作用。

〔性質３－８〕解離作用は、a'，b'，c'，d'，e'，f'，g' & g"形に分類される。

解離原理と解離作用との基本的関係が、次の構成則として得られる：

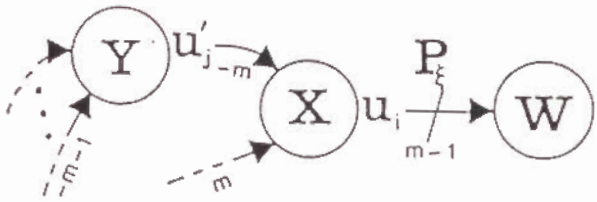
［構成則３－２］解離原理P_1，P_2，P_3は、a'，b'，c'，d'，e'（および／または）f'の解離作用により実現され、解離原理P_4は、g' & g"形の解離作用によってのみ実現される。

図３－１は、単一の解離作用による解離の図式表現である。解離形１は解離原理P_1，P_2，P_3を、解離形２は解離原理P_4を表している（$u_1' \equiv a'$，$u_2' \equiv b'$，$u_3' \equiv c'$，$u_4' \equiv d'$，$u_5' \equiv e'$，$u_6' \equiv f'$；$u_1 \equiv a$，$u_2 \equiv b$，$u_3 \equiv c$，$u_4 \equiv d$，$u_5 \equiv e$，$u_6 \equiv f$：アークと作用記号で作用鎖を表す）。アーク下部の"-m"及び"-m+1"（m=1,2,3,･･･）は直接原因作用鎖（m=0）からの連鎖順位に"-1"を乗じた値を示す。解離とその原理が作用鎖上にスラッシュ（／）と記号P_ξ（$\xi \in 1,2,3,4$）を付記することにより示される。

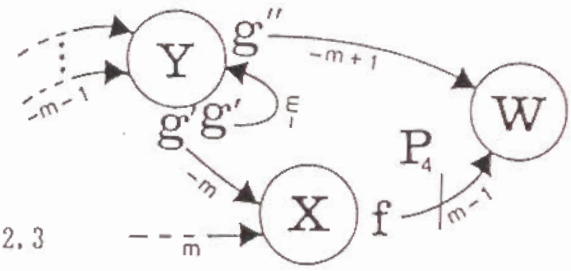
３．３．２　制御連鎖と抑制作用

解離作用を発生させるためには、一般に、解離要素に結合する、ある種の作用連鎖が生成されることが必要である。

［解離形　1］



［解離形　2］



i∈1,2,3,4,5,6　　j∈1,2,3,4,5,6　　ξ∈1,2,3

$u_1 \equiv a$,　$u_2 \equiv b$,　$u_3 \equiv c$,　$u_4 \equiv d$,　$u_5 \equiv e$

$u_1' \equiv a'$, $u_2' \equiv b'$, $u_3' \equiv c'$, $u_4' \equiv d'$, $u_5' \equiv e'$, $u_6' \equiv f'$

図３－１　解離の図式表現

［定義３－１６］解離要素に結合し、解離作用の発生の必要条件となる作用連鎖を抑制連鎖、抑制連鎖の生成の必要条件となる作用を抑制作用、そして抑制作用を発生する要素を抑制要素と言う。

［定義３－１７］解離作用鎖と、その抑制連鎖からなる単連鎖を、制御連鎖と言う。

｛性質３－９｝制御連鎖は、一方の端から解離作用鎖まで次々と連鎖する抑制作用鎖と、その解離作用鎖からなる単連鎖であり、各々の抑制作用鎖は、その次の抑制または解離作用鎖の必要条件となっている。

｛性質３－１０｝解離作用の発生には、必要とされる全ての制御連鎖、従って全ての抑制連鎖が生成されなければならない。

［定義３－１８］ある解離に必要な制御連鎖の集合を、その解離に関する潜在危険制御系と言う。

［定義３－１９］抑制作用を次のように分類する：

ａ”．エネルギ伝播形：エネルギの授受が行われることにより生ずる抑制作用。

ｂ”．情報伝達形：情報量として意味をもつ働きが行われることにより生ずる抑制作用。

ｃ”．作因物転移形：物質として認識可能な作因物の授受により生ずる抑制作用。

ｄ”．供給阻止形：必要とされる供給を阻止することにより生ずる抑制作用。

ｅ”．存在形態形：エネルギの伝播、情報の伝達、作因物の転移を伴わず、それらの供給を阻止するものでもないｆ”形以外の抑制作用。

ｆ”．機能停止形：抑制要素が能動的な状態にあることにより行われる機能を停止することにより生ずる抑制作用。

｛性質３－１１｝抑制作用はａ”，ｂ”，ｃ”，ｄ”，ｅ”，ｆ”形に分類される。

３．３．３　制御連鎖の反転と反転連鎖の解離

｛性質３－１２｝要素から抑制または解離作用が生成されないことにより、あ

る種の作用が生ずる。

［定義３－２０］抑制または解離作用が生成されないことにより生ずる作用を、反転作用と言い、またそのとき抑制または解離作用鎖が反転したと言う。

［定義３－２１］反転作用を、次のように分類する：

$\overline{a}$．エネルギ伝播形：エネルギの授受が行われることにより生ずる反転作用。

$\overline{b}$．情報伝達形：情報量として意味をもつ働きが行われることにより生ずる反転作用。

$\overline{c}$．作因物転移形：物質として認識可能な作因物の授受が行われることにより生ずる反転作用。

$\overline{d}$．供給阻害形：必要とする供給を阻害することにより生ずる反転作用。

$\overline{e}$．存在形態形：エネルギの伝播、情報の伝達、作因物の転移を伴わず、それらの供給を阻害するものでもない$\overline{f}$形以外の反転作用。

$\overline{f}$．機能不履行形：はたすべき機能を行なわないことによる反転作用。

｛性質３－１３｝反転作用は、$\overline{a}$，$\overline{b}$，$\overline{c}$，$\overline{d}$，$\overline{e}$，$\overline{f}$形に分類される。

解離、抑制および反転作用においても、作用の場合と同様に、f'、f"または$\overline{f}$形以外の解離、抑制または反転作用を、それぞれ能動形解離作用、能動形抑制作用または能動形反転作用として分類できる。

抑制および解離作用の反転と反転作用との関係が次のように得られる：

［構成則３－３］能動（a'，b'，c'，d'，e'，g' & g"）形の解離作用または能動（a"，b"，c"，d"，e"）形の抑制作用が反転すると機能不履行（$\overline{f}$）形の反転作用が生じ、f'（f"）形の解離（抑制）作用が反転すると能動（$\overline{a}$，$\overline{b}$，$\overline{c}$，$\overline{d}$，$\overline{e}$）形の反転作用のうち少なくともひとつが生ずる。

｛性質３－１４｝ある要素からの抑制または解離作用鎖は：１）その要素へ結合する抑制作用鎖が反転する、または、２）その要素に抑制または解離作用を反転させる変化が生ずる；ことによって反転する。

［定義３－２２］ある要素に生ずる変化のうち：１）その要素へ反転作用鎖が結合していない条件下で、その要素からの抑制または解離作用鎖を反転させる

もの、または、２）その要素へ解離作用が結合していない条件下で、その要素からの反転作用を元の抑制または解離作用鎖へ再反転させるもの；を引金変化という。

抑制作用鎖の反転と反転連鎖との関係が次のように得られる：

［構成則３－４］抑制連鎖を構成する任意の要素に引金変化が発生すると、他に引金変化が発生していない条件下で、その要素からの抑制作用鎖が反転することにより、そこから反転連鎖が生成され、解離は実現されない。

反転作用の性質は、作用連鎖を構成する作用の性質と同じで、反転作用の解離と解離原理との関係は次のようになる：

［構成則３－５］能動（$\overline{a}$，$\overline{b}$，$\overline{c}$，$\overline{d}$，$\overline{e}$）形の反転作用鎖は解離原理P_1，P_2またはP_3によって、$\overline{f}$形の反転作用鎖は解離原理P_4によってのみ解離される。

反転作用鎖の解離と制御連鎖の復活との基本的関係が次のように得られる：

［構成則３－６］構成則３－４において生じた反転連鎖中のある反転作用鎖が解離されると、他に引金変化および反転連鎖が生じていない条件下で、そこから部分的に抑制連鎖が復活し、作用連鎖の解離が再び可能となる。

３．３．４　抑制および解離作用の定量的性質

潜在危険制御系の設計では、抑制および解離作用の定量的な性質がしばしば重要な意味を持つ。例えば、抑制作用鎖［$Yu_i{}''\xrightarrow{n}$］においては、抑制作用$u_i{}''$が複方向（例えば信号が０と１の両方向）に制御される場合と、（信号が０または１のみの）単方向にのみ制御されるものとでは重要な相違が生ずる。これに関して、まず次の定義を行う。

［定義３－２３］作用の性質や強度が、単一の方向に変動することにより実現される抑制または解離作用鎖を、単方向制御作用鎖、複方向に変動制御されることにより実現されるものを、複方向制御作用鎖と言う。

［定義３－２４］潜在危険制御系に、複数の複方向制御作用鎖があり、一方の作用の制御の変動方向が、他方の変動方向に依存するとき、前者を外依複方向

作用鎖と言う。

〔性質３－１５〕潜在危険制御系に外依複方向作用鎖が存在するとき、それとそれが依存する複方向制御作用鎖を結ぶ、複方向制御作用鎖からなる抑制連鎖が存在しなければならない。

解離要素または抑制要素が複方向制御作用を発生するためには、要素がその作用に関して能動的な状態になければならない。他方、単方向制御作用は、要素が能動的な状態またはそれ以外のいずれの状態からも生成され得る。従って単方向または複方向制御作用と、それを構成する解離（抑制）作用との関係が次のように得られる：

［構成則３－７］単方向制御作用鎖は任意の解離または抑制作用鎖によって構成され得るが、複方向制御作用鎖はｆ’（ｆ”）形の解離（抑制）作用鎖では構成できない。

３．３．５　被制御要素の状態遷移

潜在危険は、潜在危険制御系が被制御要素のエネルギ状態や化学的性質を制御する、すなわち作用鎖（反転作用鎖）を解離することにより抑制される。ある作用鎖が発現しようとするとき、例えば潜在危険制御系が被制御要素のエネルギ状態を高エネルギ状態Ｈから低エネルギ状態Ｌに移行させることにより作用鎖を解離させるとき：

（１）図３－２（ａ）に示すように、予め予定されていたある時間内とエネルギ・レベル内で無秩序にＨからＬに遷移させればよい；

（２）図中（ｂ）のように、ある時間内で、例えばフィードバック制御によって、外乱などに応じて定まるポイントＡ，Ｂ，‥‥などを通過させるなど、秩序をもって遷移させなければならない；

場合とがある。前者には、プラント容器のリリーフ弁開閉前後における、容器内の内部エネルギの状態遷移が典型的な例としてあげられる。後者には、気象学的外乱下での、航空機の着陸時における機体の運動エネルギの状態遷移が典型的な例としてあげられる。

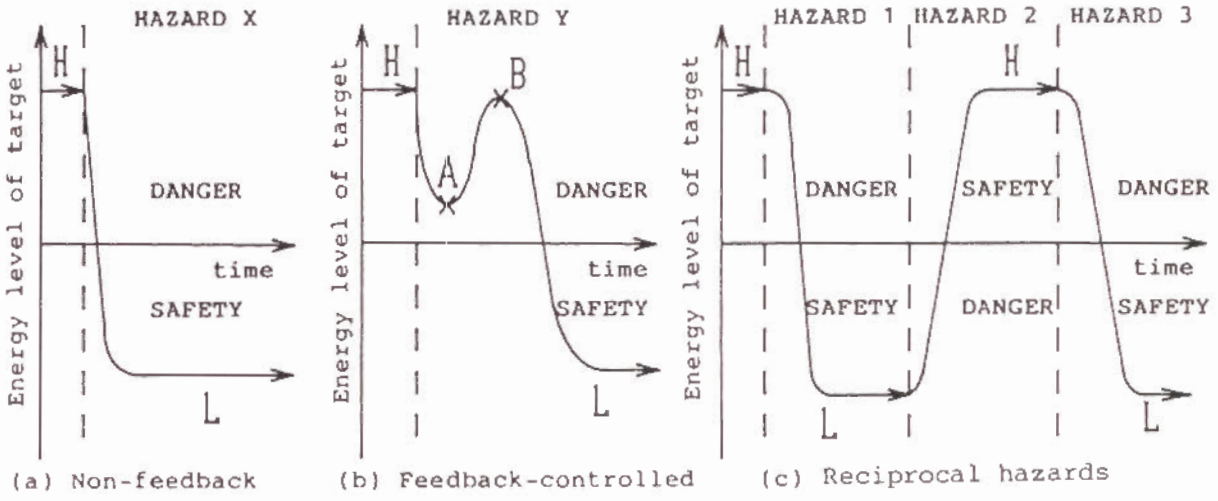


図３－２　危険回避のための被制御要素の状態遷移

無秩序な状態遷移は原理的に単方向制御作用鎖からなる潜在危険制御系でも遂行されうるが、フィードバック制御などのような秩序を持った状態遷移は、外依複方向作用鎖が必要となるため、単方向制御作用鎖のみで構成される潜在危険制御系では実現できない。従って、要素の状態遷移と制御作用鎖との関係が次のように得られる：

［構成則３－８］無秩序な状態遷移は、単方向制御作用鎖のみで構成される潜在危険制御系で原理的に実現可能である。他方、フィードバック制御による状態遷移は、外依複方向作用鎖で構成される制御連鎖を含む潜在危険制御系によてのみ実現される。

［定義３－２５］図３－２（ｃ）に示すように、系で複数の潜在危険が次々と発現しようとし、しかも潜在危険制御系による要素の状態遷移の方向が各潜在危険で異なる系がある。このような潜在危険を相反潜在危険と呼ぶ。

ｆ”（ｆ’）の作用鎖は、１方向のみの状態遷移を可能とするので、相反潜在危険に関して次の構成則を得る：

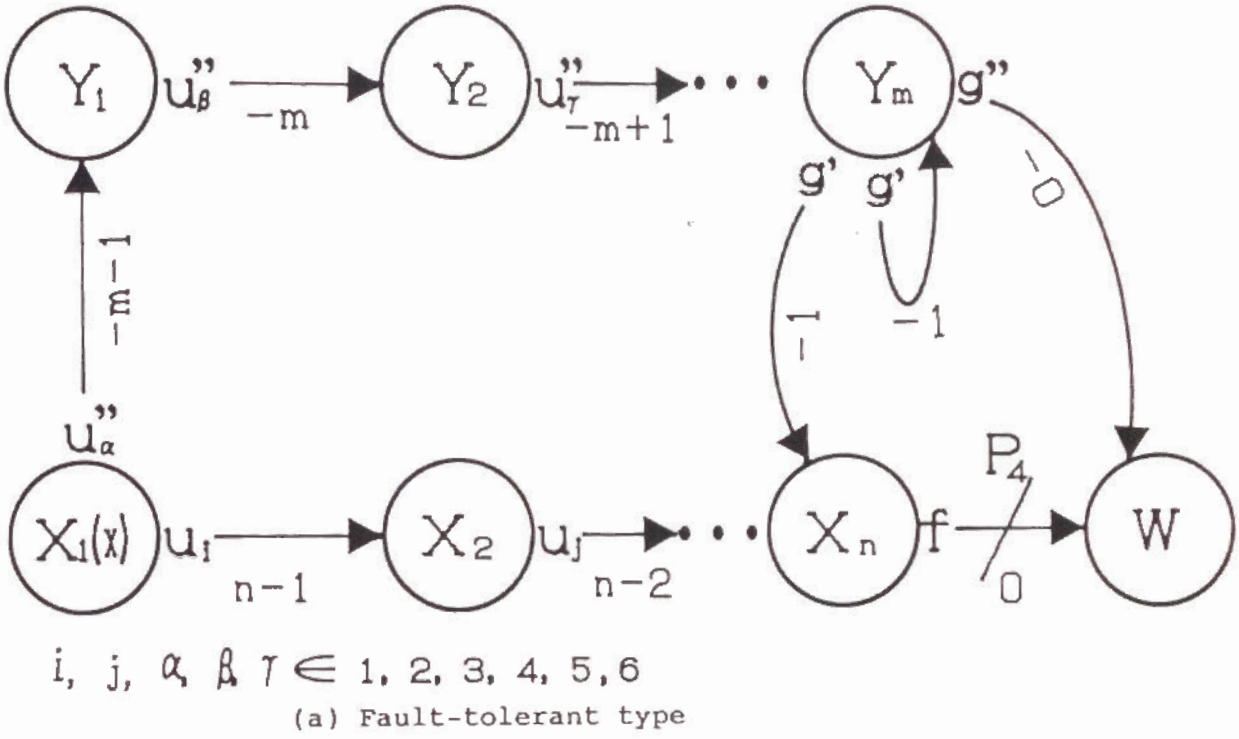
［構成則３－９］潜在危険制御系の構成要素のうち、相反潜在危険に共通して対応しなければならない要素は、少なくとも一方の潜在危険に対して能動形抑制（解離）作用鎖を構成しなければならない。

３．３．６　フェイル・セーフ・システムの構成条件

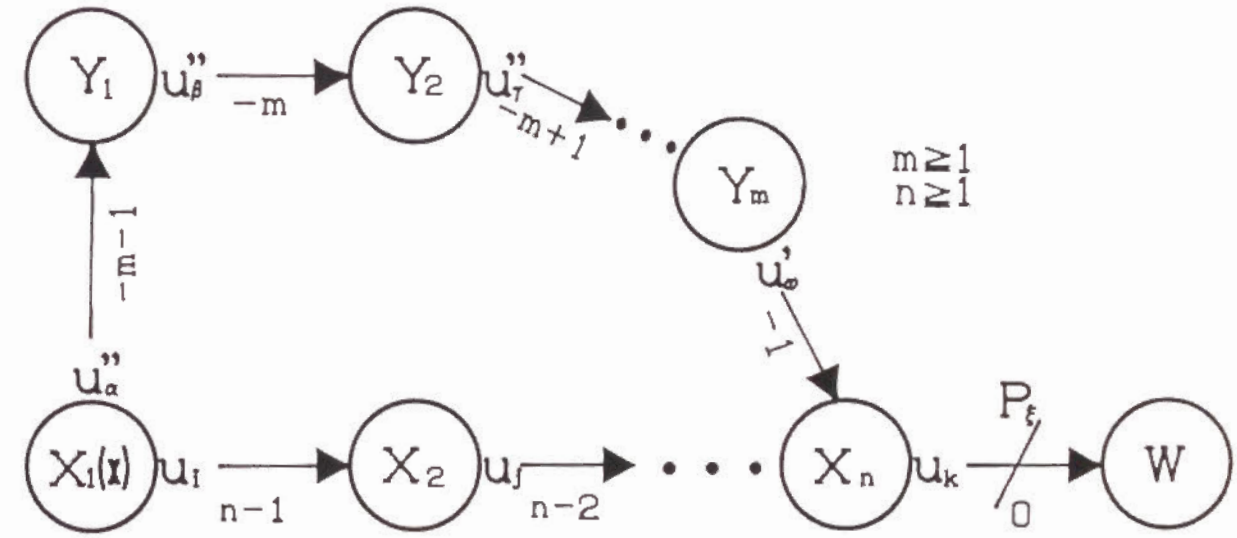
図３－３は、ある毀損を要素Ｗに生じさせる潜在危険が、要素X_1の故障ｘをひき金として、X_1、X_2、・・・と次々と作用を伝播させることにより発現しようとするとき、潜在危険制御系が作用連鎖を途中で解離して毀損を防ぐ場合の図式表現である。図中（ａ）では、作用鎖［ｆ $\xrightarrow{0}$ ］が解離原理P_4で、（ｂ）では、作用鎖［u_ξ $\xrightarrow{0}$ ］が解離原理P_ξ（$\xi \in 1,2,3$）で解離されている［構成則１、２］。

ここで、フォールト・トレラント・システムとフェイル・セーフ・システムを次のように定義する：

［定義３－２６］ある変化（故障）集合ｘの任意の変化（故障）x_iが系に発



(a) Fault-tolerant type



(b) Fail-safe type

図３－３　フェイル・セーフとフォールト・トレラント形解離を行う潜在危険制御系の図式表現

生することにより発現する作用連鎖、または、変化（故障）集合yの任意の変化（故障） y_i が系に発生することにより発現する反転連鎖を、解離原理 P_4 で解離して毀損を防止できれば、系はxとその毀損、または、yとその毀損に関してフォールト・トレラント・システムである。また、解離原理 P_4 による解離をフォールト・トレラント形解離という。

［定義３－２７］同様に、解離原理 P_ξ （$\xi \in 1,2,3$ ）で解離して毀損を防止できれば、系はxとその毀損、または、yとその毀損に関してフェイル・セーフ・システムである。また、これらの解離をフェイル・セーフ形解離という。

ここで、図３－３の抑制要素 Y_2 をセンサ、処理部および出力部などから構成される情報処理系と仮定しても一般性は失われない。故障 y_j （$\in y$）が情報処理系に発生して、［Y_2 u_γ ” $\xrightarrow{-m+1}$］が［$Y_2(y_j)$ $\bar{u}_l$ $\xrightarrow{m-1}$］と反転する場合を考える。u_γ ” が能動形（$\gamma \in 1,2,\cdots,5$ ）のとき、$\bar{u}_l$ は $\bar{f}$ となり、u_γ ” が f ” のとき能動形反転作用 $\bar{u}_l$ （$l \in 1,2,\cdots,5$ ）の少なくともひとつが生ずる［構成則３－３］。これらの反転作用のうち、能動形反転作用はフェイル・セーフ形解離で解離される［構成則３－５、定義３－２７］もし解離されるならば、情報処理系は故障yと毀損に関してフェイル・セーフシステムである。このようにして、情報処理系の構成条件に関して次の構成則を得る：

［構成則３－１０］機能停止形の抑制（解離）作用を行う情報処理系にはフェイル・セーフ・システムが、能動形抑制（解離）作用を行う情報処理系にはフォールト・トレラント・システムがそれぞれ原理的に構成可能である。

これより、次の定義を行う：

［定義３－２８］能動形抑制（解離）作用を行う情報処理系を可フォールト・トレラント情報処理系と言う。

［定義３－２９］f ” （f ’）形の作用を行う情報処理系を可フェイル・セーフ情報処理系と言う。

前節で述べた図３－２（ｂ）のフィードバック回路を構成する外依複方向制御作用鎖は、能動形抑制作用鎖のみで構成される［構成則３－７］。従って、

構成則３－１０より、フィードバック回路を機能させる情報処理系には可フォールト・トレラント情報処理系を構成しなければならない。

また、図３－２（ｃ）のような相反潜在危険に対処する潜在危険制御系が単一の情報処理系で構成される場合、その情報処理系は少なくとも１つの潜在危険に対して可フォールト・トレラント情報処理系を構成する必要がある。

３．４　移動ロボットにおける潜在危険制御系の構成事例

潜在危険制御系の重要な要素であるセンサや信号処理部などからなるいわゆる情報処理系は、基本的に可フェイル・セーフ情報処理系または可フォールト・トレラント情報処理系として構成できる［構成則３－１０］。

しかしながら、両構成法では、安全性の観点から大きな相違がある。前者は、いわゆる情報処理系に非対称故障率を持つ論理素子を適用したいわゆる狭義のフェイル・セーフ・システムの構成法となり、後者では多重・冗長設計などによる機能維持が基本となる。

狭義のフェイル・セーフ・システムは、一般的に、フォールト・トレラント・システムに比して、構造が単純で、冗長系の同時故障を考慮する必要性が少ないなど、安全上優れた特質を有している。しかし、どちらの情報処理系を採用するかなどは、対象とする潜在危険と系の全体的構造に依存しており、それらの潜在危険制御系への構成法則が前節までに体系化された。

本節では、自律移動ロボットの潜在危険のうち主要なもの２種類を取りあげ、それらに対する潜在危険制御系の構成について論ずる。

３．４．１　系を構成する要素記号の定義

Ｒ：知能移動ロボット

ＳＴ：Ｒの構造系要素

ＥＳ：Ｒの動力源

ＳＥ：Ｒの外界センサ系

ＳＩ：Ｒの内界センサ系

ＣＰ：Ｒの情報処理系処理部

ＣＡ：Ｒの情報処理系出力部

ＤＲ：Ｒの駆動部

ＢＲ：Ｒの制動部

ＳＲ：Ｒの操舵部

ＢＬ：Ｒの平衡機能系

ＴＲ：Ｒの移動機能系

ＲＳ：Ｒの滑り状態

ＲＢ：Ｒの平衡状態

ＲＭ：Ｒの運動状態

Ｏ：静止対象物

Ｍ：移動対象物

Ｇ：重力

Ｄ：路面状態などの外乱要素

Ｓ：スキッド促進要因

Ｔ：転倒促進要因

３．４．２　潜在危険の同定

知能移動ロボットには第２章で述べたような多様な潜在危険が同定される。ここで、ロボットが自律的移動を行う過程で：(i) 静止対象物Ｏと衝突する、(ii)移動する対象物Ｍが衝突する；の各潜在危険は、Ａ－Ｃモデルによりそれぞれ図３－４および図３－５のように同定される。

図３－４では、情報処理系出力部CAが駆動部DRをロボットの移動側に制御する［CAa $\xrightarrow[4]{}$］ことにより、駆動部が動力源ESから駆動のためのエネルギを受け入れる状態となり［DRe $\xrightarrow[3]{}$］、動力源ESから駆動エネルギが伝播され［ESa $\xrightarrow[2]{}$］、駆動部がロボットを動作させる［DRa $\xrightarrow[1]{}$］。このとき、対象物Ｏ

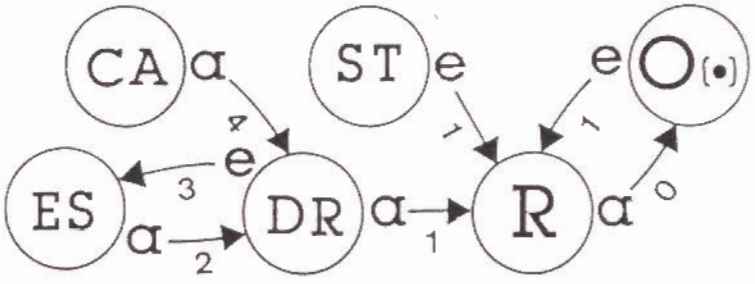


図３－４　潜在危険（１）の同定

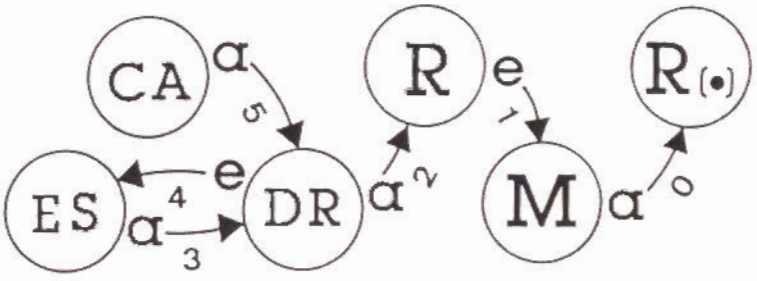


図３－５　潜在危険（２）の同定

が移動経路上に存在する［Oe $\xrightarrow{1}$］ため、ロボットが対象物と衝突し［Ra$\xrightarrow{0}$］、ロボットの構造STが十分強靭である［Re $\xrightarrow{1}$］ので毀損(・) が生ずる。

図３－５では、情報処理系の出力部が駆動部をロボットの移動側に制御する［CAa $\xrightarrow{5}$］することにより、駆動部が動力源ESから駆動のためのエネルギを受け入れる状態となり［DRe $\xrightarrow{4}$］、動力源から駆動エネルギが伝播され［ESa $\xrightarrow{3}$］、駆動部がロボットを作用させる［DRa $\xrightarrow{2}$］。このため、ロボットは移動対象物Mの移動経路に存在する［Re $\xrightarrow{1}$］こととなり、移動対象物と衝突して、毀損(・) が生ずる。ここでは、系の初期状態として、ロボットが移動対象物と衝突する可能性のない場所に存在していることを仮定している。

図３－４または図３－５に示される作用連鎖で同定される潜在危険を、それぞれ潜在危険(1) および潜在危険(2) と定義する。

３．４．３　潜在危険抑制原理(3) の適用

（ｉ）　潜在危険(1)

系の相は：ロボットの(イ) 停止モード、(ロ) 運動モード；とに分割される。すると、潜在危険抑制原理(3) 、すなわち系の相が(イ) から(ロ) へと遷移するのを禁止する潜在危険抑制措置が、次ぎのように実現される。

自律的運動の結果生ずる衝突のみを考えているので、図３－４において誘因作用鎖［DRa $\xrightarrow{1}$］，［ESa $\xrightarrow{2}$］，［DRe $\xrightarrow{3}$］は、［Ra $\xrightarrow{0}$］の必要条件となっている。誘因作用鎖［DRe $\xrightarrow{3}$］は、解離原理P_1で原理的に解離可能である［構成則３－１］。

動力源遮断インターロッキング機構が、次の制御連鎖などからなる潜在危険制御系として構成される［構成則３－２］：

$$Ou_i'' \xrightarrow{-7} SEu_j'' \xrightarrow{-6} CPu_k'' \xrightarrow{-5}$$

$$\xrightarrow{P_1}$$

$$CAu_l' \xrightarrow{-4} DRe \not\xrightarrow{3} ES \qquad (3-1)$$

解離作用鎖［CA u_i ' $\xrightarrow{-4}$］は、動力源の遮断方向のみの単方向制御作用鎖として構成でき、他の抑制作用鎖も同様である。この潜在危険制御系は可フェイル・セーフ情報処理系構成の必要条件を満足する［構成則３－１０］。

制御連鎖(3-1) に可フェイル・セーフ情報処理系を構成すると、

$$O\,u_i\,'' \xrightarrow{-7} SE\,f'' \xrightarrow{-6} CP\,f'' \xrightarrow{-5} \overset{P_1}{\underset{CA\,f' \xrightarrow{-4} DR\,e \not\xrightarrow{-3} ES}{}} \qquad (3-2)$$

可フォールト・トレラント情報処理系を構成すると、

$$O\,u_i\,'' \xrightarrow{-7} SE\,b'' \xrightarrow{-6} CP\,b'' \xrightarrow{-5} \overset{P_1}{\underset{CA\,a' \xrightarrow{-4} DR\,e \not\xrightarrow{-3} ES}{}} \qquad (3-3)$$

これらの情報処理系は、共に作用鎖［e $\xrightarrow{-3}$］を解離原理 P_1 で解離している点は同様であるが、例えばCPに変化（故障） x_1 と x_2 がそれぞれ発生すると、(3-2) と(3-3) は、それぞれ

$$O\,u_i\,'' \xrightarrow{-7} SE\,f'' \xrightarrow{-6} CP\,(x_1)\,\overline{b} \xrightarrow{-5} \qquad CA\,\overline{b} \xrightarrow{-4} DR\,e \xrightarrow{-3} ES \qquad (3-2)'$$

$$O\,u_i\,'' \xrightarrow{-7} SE\,b'' \xrightarrow{-6} CP\,(x_2)\,\overline{f} \xrightarrow{-5} \qquad CA\,\overline{f} \xrightarrow{-4} DR\,e \xrightarrow{-3} ES \qquad (3-3)'$$

と反転連鎖を形成して解離が実現されなくなる［構成則３－３］。

ここで、反転連鎖（３－２）’における反転作用鎖［$\overline{b} \xrightarrow{-5}$］は、$x_1$に対するフェイル・セーフ機構によるフェイルセーフ形解離により解離され、反転連鎖（３－３）’における反転作用鎖［$\overline{f} \xrightarrow{-5}$］は、$x_2$に対するフォールト・トレラント機構によるフォールト・トレラント形解離により解離される［構成則３－５］。もし、それらの反転作用鎖が解離されれば、再び元の作用鎖の解離が可能となる［構成則３－６］。

図３－６には、可フェイル・セーフ情報処理系を用いた潜在危険制御系を概念化する。ここで、ST_2は情報処理系出力部の構造系下位要素、ES_1は駆動部の制御系下位要素の動力源である。

ロボットが移動し始めようとしたとき、対象物の存在形態形作用［Oe" $\xrightarrow{-9}$］により外界センサ、処理部、出力部が次々と出力機能を停止する。すると駆動部は、その制御系下位要素の動力源ES_1が作用する状態に移行し［DRe" $\xrightarrow{-5}$］、ES_1が駆動部に作用して［ES_1 a’ $\xrightarrow{-4}$］、駆動部は動力源ESから完全に遮断された状態となる。

（ii）潜在危険（２）

系の相は、ロボットが対象物Mとの干渉可能領域に：(イ) 存在しないモード、(ロ) 存在するモード；とに分割される。はじめ系の相は(イ) のモードにあってそこに留まる限りMと干渉しないことを仮定しているので、誘因作用鎖［DRe $\xrightarrow{-4}$］は直接原因作用［Ma $\xrightarrow{0}$］の必要条件となっている。直接原因作用を抑制するには［DRe $\xrightarrow{-4}$］を解離すればよいので、次の制御連鎖などからなる潜在危険制御系が構成される［構成則３－１］：

$$Mu_i" \xrightarrow{-8} SEu_j" \xrightarrow{-7} CPu_k" \xrightarrow{-6} \overset{P_1}{CAu_l'} \xrightarrow{-5} DRe \overset{P_1}{\not\xrightarrow{-4}} ES \qquad (3-4)$$

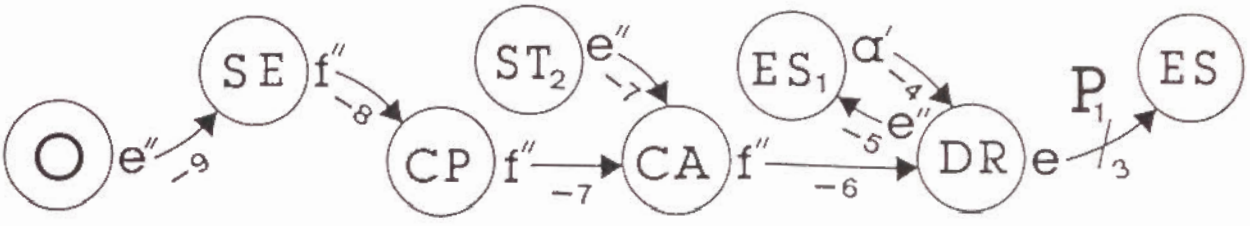


図３－６　潜在危険(1)に対して潜在危険抑制原理(3)適用の潜在危険制御系主要部(可フェイル・セーフ情報処理系)

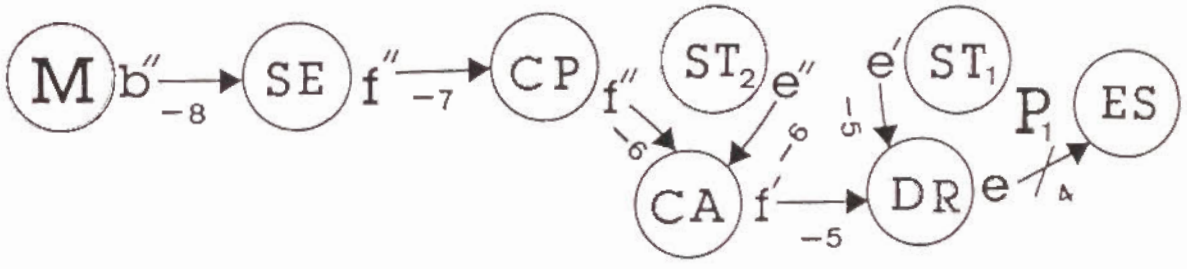


図３－７　潜在危険(2)に対して潜在危険抑制原理(3)適用の潜在危険制御系主要部(可フェイル・セーフ情報処理系)

前節と同様に、制御連鎖は動力の遮断方向のみの単方向制御作用鎖とすることができるので、可フェイル・セーフ情報処理系構成の必要条件を満足する。

図３－７には可フェイル・セーフ情報処理系を用いた潜在危険制御系を構成する。ES_2 は情報処理系の動力源、ST_2 は処理部の構造系下位要素、ST_1 は駆動部の構造系下位要素である。

ここで、センサは、抑制作用 u_i'' が f'' のとき、移動対象物がロボットと干渉しない空間に存在することを常時監視する機構となり、それ以外では、移動対象物がロボットと干渉する空間に存在することを検出する機構となる。

３．４．４　潜在危険(1) に対する潜在危険抑制原理(4) の適用

ここで、系の相がすでにロボットの運動モードに遷移した後の潜在危険制御系を検討する。

（ｉ）　制動制御衝突回避

（i-１）　単純制動衝突回避

直接原因作用鎖［$Ra \xrightarrow{0}$］は原理的に解離原理 P_1 によって解離可能である［構成則３－１］。すなわち、ロボットを停止させたときに他の潜在危険が生じないとき、次の制御連鎖からなる潜在危険制御系が構成される［構成則３－２］：

$$O\,u_i'' \xrightarrow{-5} SE\,u_j'' \xrightarrow{-4} CP\,u_k'' \xrightarrow{-3}$$

$$CA\,u_l'' \xrightarrow{-2} BR\,u_m' \xrightarrow{-1} Ra \overset{P_1}{\not\longrightarrow_{0}} O \qquad (3-5)$$

制御連鎖は停止方向のみの単方向制御作用鎖で構成可能で、可フェイル・セフ情報処理系を構成する必要条件を満足する［構成則３－１０］。

図３－８には、可フェイル・セーフ情報処理系を用いた潜在危険制御系が構成されている。ここで、ST_3 と ES_3 はそれぞれ制動部の構造系下位要素と制動部の制御系下位要素の駆動エネルギ源である。対象物からの存在形態形抑制作

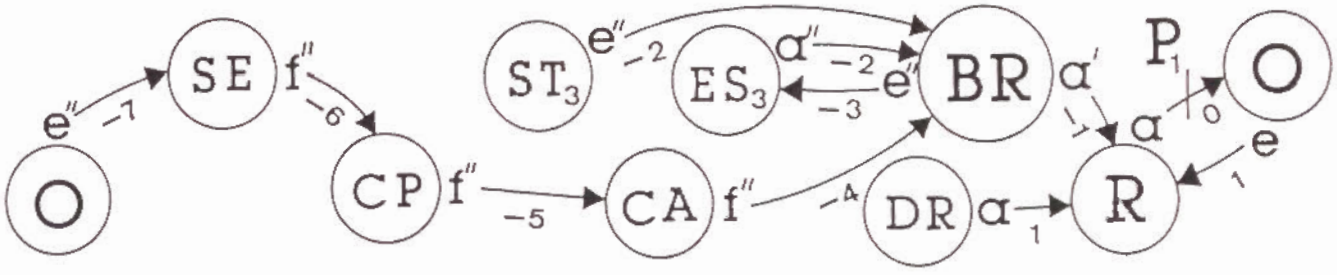


図３－８　潜在危険(1)に対する単純制動衝突回避潜在危険制御系主要部(可フェイル・セーフ情報処理系)

用によって、外界センサ、処理部、出力部が次々と出力を停止し、制動部がロボットの運動エネルギを熱または電気的エネルギなどに変換する。こうして、ロボットが停止する。

（i-2）　スキッドが生ずる系

ロボットの構造や環境条件によっては制動に伴いスキッドが発生し、結果的に衝突が生ずる潜在危険（図３－９）を考慮する必要がある。これは、ロボットの足場の状態などスキッド促進作用［$Se \xrightarrow{-2}$］と制動力［$BRe \xrightarrow{-2}$］により、制動部がロックされ［BR(1)］、ロボットの制動に失敗するものである。

スキッドへの対抗手段として、滑りを検出して制動力をON-OFF制御する方法が考えられる[75]。すなわち、作用鎖［$BRe \xrightarrow{-2}$］は、解離原理P_1で解離可能で、次の制御連鎖などからなる潜在危険制御系が構成される：

$$RSu_i'' \xrightarrow{-6} SIu_j'' \xrightarrow{-5} CPu_k'' \xrightarrow{-4} \overset{P_1}{\cdots} CAu_l' \xrightarrow{-3} BRe \not\xrightarrow{-2} BR \qquad (3-6)$$

ここで解離作用鎖［$CAu_l' \xrightarrow{-3}$］は、滑り状態からの抑制作用［$RSu_i'' \xrightarrow{-6}$］に従って制動力のON-OFF制御を行うので外依複方向制御作用鎖となり、制御連鎖(3-6) 以外にこれらを結ぶ抑制連鎖が存在しない条件下で、制御連鎖(3-6) を構成する抑制作用鎖は全て複方向作用鎖となる〔性質３－１５〕。

従って、制御連鎖(3-6) に対しては、可フェイル・セーフ情報処理系を構成することができない［構成則３－７，３－１０］。

図３－１０のような潜在危険制御系が概念化される。ここでSI_1はスキッド検出センサ、ES_2は情報処理系の動力源、ES_3は制動部駆動エネルギ源である。

連鎖順位を示す数字に＊印を付した制御連鎖がスキッド制御系である。処理部は、外界センサからの抑制作用［$SEf'' \xrightarrow{-6}$］とスキッド検出センサからの出力［$SI_1\ b'' \xrightarrow{-5}$］に基づいて、スキッドを抑制しながら制動できるよう制

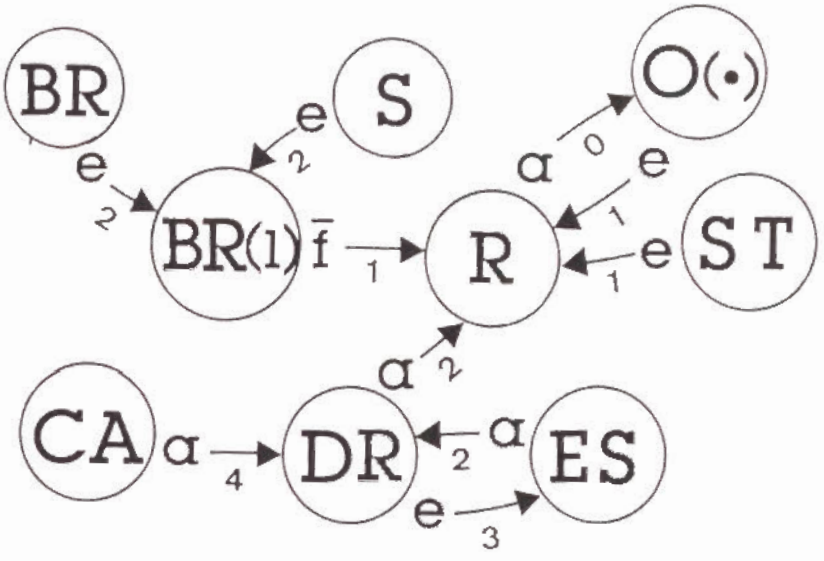


図３－９　スキッドのある潜在危険

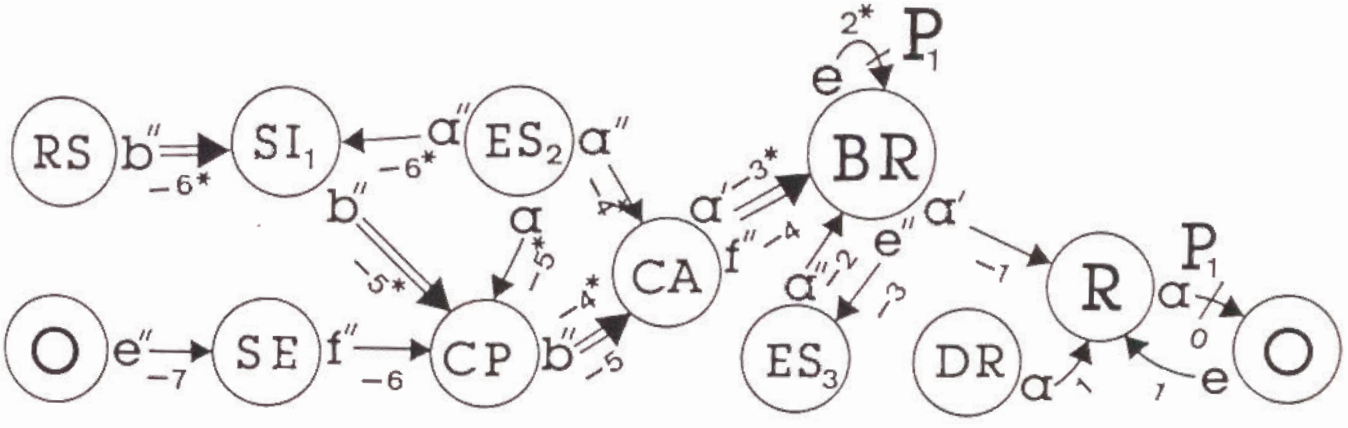


図３－１０　スキッドのある潜在危険に対する制動力のON-OFF制御衝突回避潜在危険制御系主要部

動力制御のための演算処理を行い、出力部を通じて制動力を制御することによりロボットを停止させる。

図中、２重アークは、その作用鎖が複方向作用鎖であることを示す。

（i-３）　転倒が生ずる系

２足歩行ロボットなどは、不規則な形状をもつ足場などからの外乱により、停止時に平衡を失い転倒することがある。転倒により、ロボットと対象物Ｏとの衝突潜在危険が図３－１１のように発現する。従って、このようなロボットでは、転倒を防止するための平衡制御を行う必要がある。

外乱Ｄやロボットの平衡状態RBを検出し、制動や駆動制御を行って転倒を抑制しながらロボットを停止させる潜在危険制御系が考えられる。これを実現するため、次のような制御連鎖を構成する：

$$Y_{1,i}\ u_{\xi(i)}'' \xrightarrow{-6} Y_{2,i}\ u_{\eta(i)}'' \xrightarrow{-5} CP\,u_j'' \xrightarrow{-4} CA\,u_k'' \xrightarrow{-3} P_1$$

$$Y_{5,i}\ u_{\zeta(l)}'' \xrightarrow{-2} BL\,u_m' \xrightarrow{-1} Ra \not\xrightarrow{0} O \qquad (3-7)$$

$i,l \in 1,2$　　$\xi_{(i)}$, $\eta_{(i)}$, j,k, $\zeta_{(l)}$, $m \in 1,2,3,\cdots\cdots,6$

$Y_{1,1} \equiv D$,　$Y_{1,2} \equiv RB$,　$Y_{2,1} \equiv SE_1$,　$Y_{2,2} \equiv SI_2$,

$Y_{5,1} \equiv BR$,　$Y_{5,2} \equiv DR$

ここでSE_1 は外乱検出センサ、SI_2 は平衡状態検出センサである。

$[Y_{5,l}\ u_{\zeta(l)}'' \xrightarrow{-2}]$ (l=1 and/or 2)は、不規則に変化する外乱と平衡状態に対応する外依複方向制御作用鎖となる。

制御連鎖(3-7) 以外に $[Y_{5,l}\ u_{(l)}'' \xrightarrow{-2}]$ (l=1 and/or 2)と $[Y_{1,i}\ u_{(i)}'' \xrightarrow{-6}]$ (i=1 and 2) を結ぶ抑制連鎖が存在しない条件下で、抑制連鎖を構成する抑制作用鎖は全て複方向制御作用鎖となる｛性質３－１５｝。従って可フェイル・セーフ情報処理系を構成できない［構成則３－１０］。

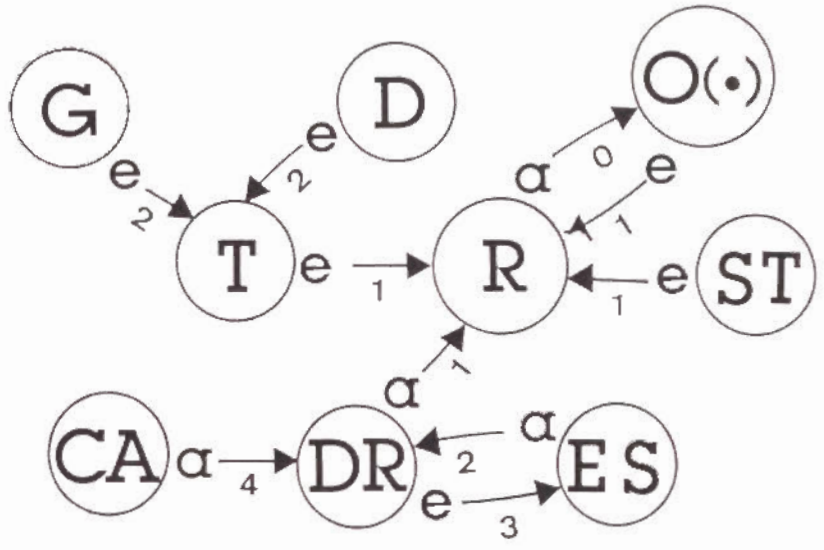


図３－１１　転倒のある潜在危険

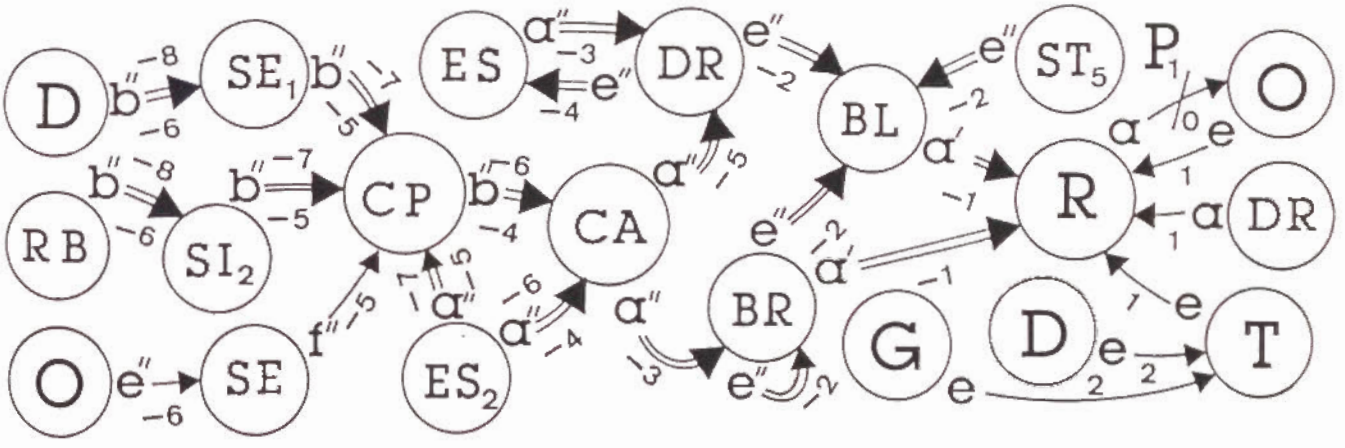


図３－１２　転倒のある潜在危険に対する多元制動制御衝突回避潜在危険制御系主要部

図３－１２に示す潜在危険制御系が構成される。ES_2 は情報処理系の動力源、ST_5 は平衡機能系の構造系下位要素である。

処理部は、外乱検出センサや平衡状態検出センサからの出力、および対象物検出センサからの抑制作用鎖［SE f $\xrightarrow{-5}$］に従って、ロボットを転倒させずに停止させるための演算処理を行い、出力部を通じて駆動部や制動部を制御しながらロボットを停止状態へと移行させる。

（ii）　経路制御衝突回避

制動衝突回避よりも経路を変更することによる衝突回避の方が現実的な場合がある。ｎ個の静止対象物O_i（$i \in 1,2,\cdots,n$）に対し、経路回避を実現する潜在危険制御系は、次の制御連鎖などから構成される：

$$O_i \; u_{\xi(i)}'' \xrightarrow{-5} SE\,u_j'' \xrightarrow{-4} CP\,u_k'' \xrightarrow{-3} CA\,u_l'' \xrightarrow{-2} P_l \; SR\,u_m' \xrightarrow{-1} Ra \not\xrightarrow{0} O_q \qquad (3-8)$$

$$i,q \in 1,2,\cdots,n \qquad \xi(i),j,k,l,m \in 1,2,\cdots,6$$

（ii－１）　単静止対象物回避系

まず、単静止対象物（１回の経路変更操作によって衝突が回避できる範囲の大きさの障害物）Ｏのみを回避すればよい系を検討する

制御連鎖（３－８）における解離作用鎖［$SR\,u_m' \xrightarrow{-1}$］は、抑制作用鎖［$O\,u_{\xi(i)}'' \xrightarrow{-5}$］に従って静止対象物から離隔する方向のみの単方向制御作用鎖とでき、単方向制御作用鎖からなる制御連鎖を構成できるので、可フェイル・セーフ情報処理系を構成する必要条件が満たされる。

可フェイル・セーフ情報処理系を用いた潜在危険制御系を図３－１３に示す。ST_4、ES_4 はそれぞれ操舵部の構造系下位要素と操舵部の制御系下位要素の駆動エネルギ源である。

対象物の存在形態形抑制作用［$O\,e'' \xrightarrow{-7}$］によって、センサ、処理部、出

力部が次々と出力を停止する。すると、操舵部は、ES_4 から最大経路変更となる操舵エネルギが操舵部へ伝播される状態へと移行し［SRe" $\xrightarrow{-3}$］、エネルギが伝播され［ESa" $\xrightarrow{-2}$］、操舵部がロボットの経路を変更する［SRa' $\xrightarrow{-1}$］。

（ii－2）　多静止対象物同時回避系

n個の単静止対象物O_i（i=1,2,･･･,n）が1回の経路変更では回避できない範囲に分布している系を想定する。

制御連鎖(3-8)における解離作用鎖［SRu_m' $\xrightarrow{-1}$］は、多対象物からの抑制作用鎖［O_i $u_{\varepsilon(i)}$" $\xrightarrow{-5}$］に従って、全ての対象物を回避できるように経路を複方向に制御しなければならないので、単方向制御作用鎖として構成できない。従って、制御連鎖(3-8)以外にそれらを結ぶ抑制連鎖が存在しない条件下で、この制御連鎖を構成する抑制作用鎖は全て複方向制御作用鎖でなければならないので可フェイル・セーフ情報処理系を構成できない。

図3－14に示す潜在危険制御系が構成される。ES_2 は情報処理系の動力源、ES_4 とST_4 はそれぞれ操舵部の駆動エネルギ源と構造系下位要素である。

外界センサ系SEが、多対象物の「大きさ・位置」などの情報を処理部に出力すると、処理部は、これに基づいて、全ての対象物に対して衝突を回避できる経路を生成するための演算処理を行い、出力部を通じて操舵部に出力する［CAa" $\xrightarrow{-4}$］。これによって操舵部が制御され、衝突を回避するロボットの経路が生成されていく。

3．4．5　潜在危険(2)に対する潜在危険抑制原理(4)の適用

潜在危険(2)において、誘因作用鎖［Re $\xrightarrow{-1}$］は直接原因作用鎖［Ma $\xrightarrow{0}$］が発現する必要条件となっている。従って、この誘因作用鎖を解離することによって直接原因作用鎖の発現を抑止することができる。

この解離は、構成則3－1より解離原理P_1、すなわちロボットが対象物Mの経路から移動・離隔することによって行われる。これを実現する潜在危険制御系は、次の制御連鎖などから構成される：

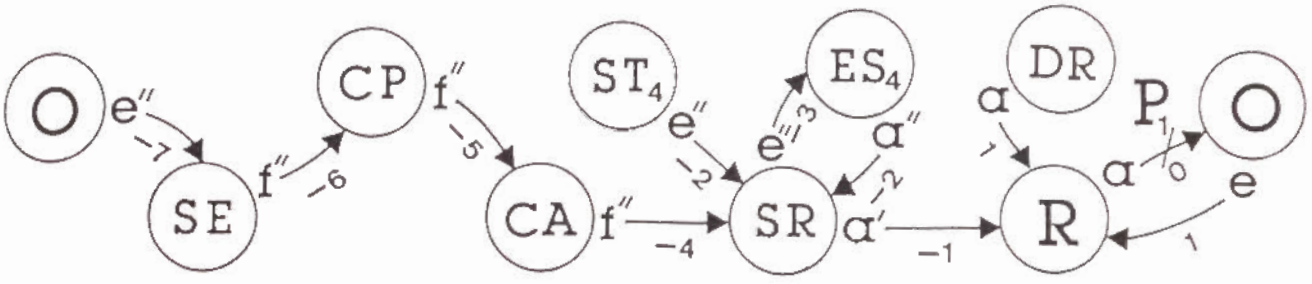


図３－１３　径路制御単静止対象物衝突回避潜在危険制御系主要部

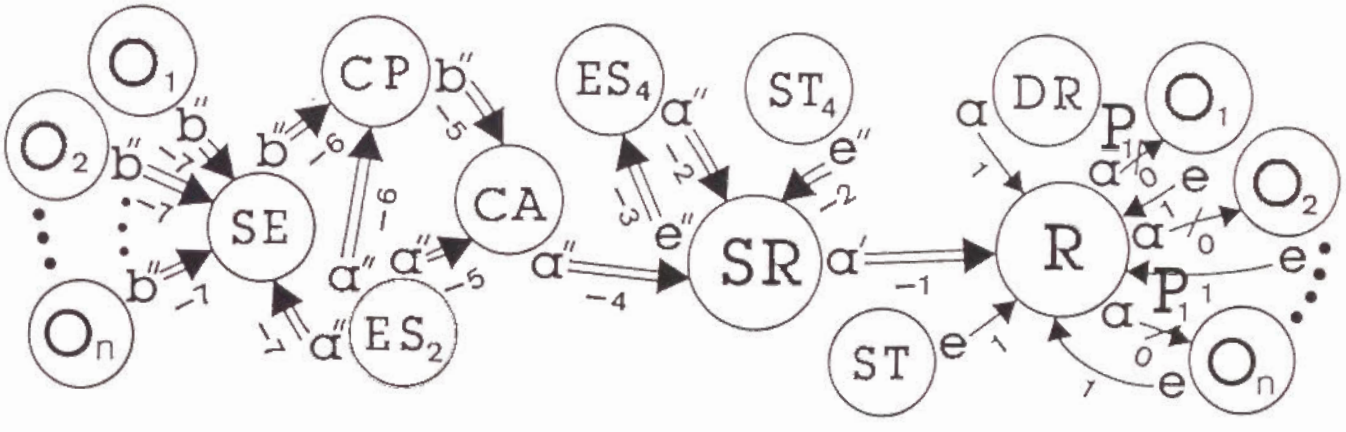


図３－１４　径路制御多静止対象物同時衝突回避潜在危険制御系主要部

$$Mu_i\,''\xrightarrow{-7}SEu_j\,''\xrightarrow{-6}CPu_k\,''\xrightarrow{-5}CAu_l\,''\xrightarrow{-4}$$

$$P_l$$

$$Y_m\ u_{\xi(m)}\,''\xrightarrow{-3}TRu_n\,'\xrightarrow{-2}Rc\xrightarrow{-1}M \qquad (3-9)$$

$$i,j,k,l,\ \xi_{(m)}\ ,n\in 1,2,\cdots,6 \qquad m\in 1,2,3$$

$$Y_1\equiv DR,\ Y_2\equiv SR,\ Y_3\equiv BR$$

一般的に、ロボットが任意の運動状態RMにあって、未知の移動経路を有する対象物Mから、その運動状態を予測して衝突を回避するには、解離作用鎖［$TRu_n\,'\xrightarrow{-2}$］が［$Mu_i\,''\xrightarrow{-7}$］に従う外依複方向作用鎖でなければならない。制御連鎖(3-9) 以外にそれらを結ぶ抑制連鎖が存在しない条件下で、この抑制連鎖を構成する抑制作用鎖は全て複方向制御作用鎖となる。従って、この潜在危険制御系に可フェイル・セーフ情報処理系を構成することはできない。

対象物Mがｎ個存在する場合の潜在危険制御系を図３－１５に構成する。

SI_3 はロボットの運動状態を検出するセンサ、ST_6 は移動機能系の構造系下位要素である。

外界センサ系SEは、対象物M_i（$i=1,2,\cdots,n$）からの情報［$M_i\ b''\xrightarrow{-7}$］に基づいて、その位置、運動方向、速度などを検出する。処理部は、外界センサとSI_3 などからの出力に基づいて、全ての対象物に対して衝突回避を実現するための移動計画生成のための演算処理を行い、出力部を通じて、駆動部、操舵部、制動部を制御する。これにより、衝突を回避するための移動機能系が発動して［$TRa'\xrightarrow{-2}$］、衝突が回避される。

３．４．６　情報処理系の適用範囲

前節までに構成された潜在危険抑制原理（４）適用の潜在危険制御系の情報処理系と、その潜在危険空間への適応範囲との関係を纏める。

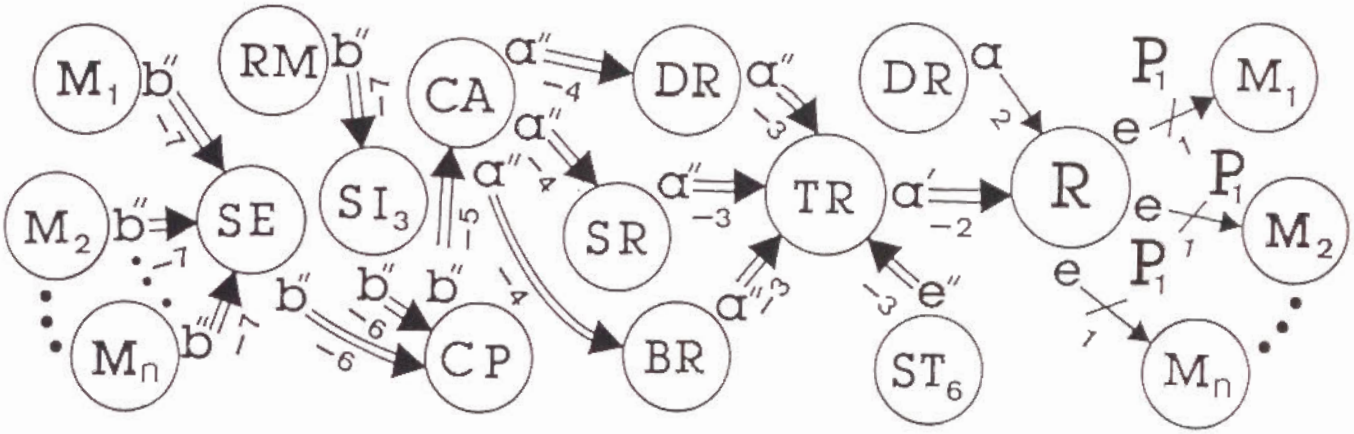


図３－１５　多元移動制御衝突回避潜在危険制御系主要部

図３－４、図３－５、図３－９または図３－１１に示される作用連鎖中の単連鎖［Ｒａ$\xrightarrow[0]{}$Ｏ（・）］および［Ｍａ$\xrightarrow[0]{}$Ｒ（・）］で同定される潜在危険集合をそれぞれH1、H2として定義する。すると、潜在危険集合H1、H2および全潜在危険集合Ｈとの関係は、図３－１６として表せる。

抑制原理（４）適用の潜在危険制御系のうち、可フェイル・セーフ情報処理系を用いたものは楕円領域Ｓ内、可フォールト・トレラント情報処理系を用いたものは楕円領域Ｄ内の潜在危険集合に対してそれぞれ適応可能である。

H1やH2で領域ＳやＤに含まれない部分は、潜在危険制御系の異常や故障などの変化により生成される潜在危険集合である。

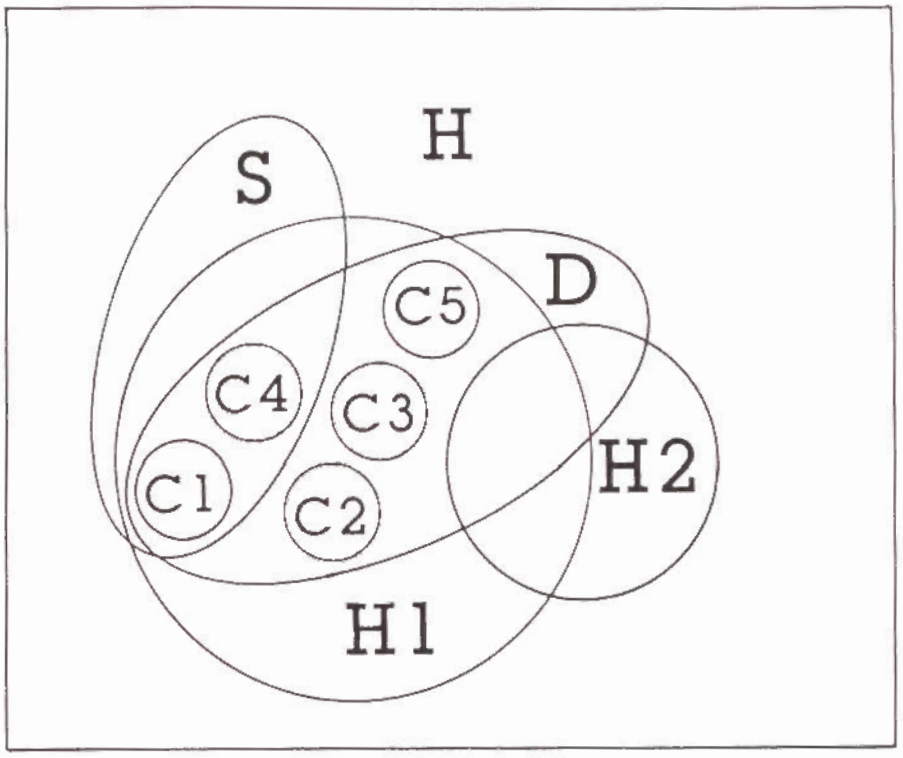
対象物Ｏとの衝突回避形式：C1（単純制動衝突回避）、C2（対スキッド制御制動衝突回避）、C3（平衡制御制動衝突回避）、C4（経路制御単静止対象物衝突回避）、C5（経路制御多静止対象物同時衝突回避）を行う各潜在危険制御系のうち、原理的に可フォールト・トレラント情報処理系で構成可能なものが領域Ｄ内に、また可フェイル・セーフ情報処理系で構成可能なもの（すなわちC1,C4）がＳ内に表示されている。

全潜在危険空間Ｈに対応できる潜在危険制御系を構成することは不可能であるから、対処すべき潜在危険の優先順位を決定するなどして、合理的に潜在危険制御系を構成していくことが必要である。

３．５　考　　察

図３－１を比較してわかるように、解離形１（解離原理P_1，P_2，P_3）すなわちフェイル・セーフ形解離原理の適用は、解離形２（解離原理P_4）すなわちフォールト・トレラント形解離原理に比し、構造が単純で、冗長系あるいは多重系の同時故障を考慮する必要性が少ないなどの利点をもつ。しかし、どちらの解離形が採用できるかは、解離しようとする作用鎖または反転作用鎖と系の構造に依存する。

3.4.3 節では処理部の故障のみを取り上げたが、実際の系では他にも多様な



領　域　　H：全潜在危険集合

円領域　　H1：潜在危険集合［Ra ⟶ H（・）］

円領域　　H2：潜在危険集合［Ma ⟶ R（・）］

楕円領域　D：可フォールト・トレラント情報処理系を用いた潜在危険抑制原理（4）適用の潜在危険制御系の潜在危険集合抑制範囲

楕円領域　S：可フェイル・セーフ情報処理系を用いた潜在危険抑制原理（4）適用の潜在危険制御系の潜在危険集合抑制範囲

図3－16　可フォールト・トレラント情報処理系と可フェイル・セーフ情報処理系から構成される潜在危険制御系の潜在危険集合への適用範囲

故障モードが存在するので、それらを全て検討する必要がある。この検討は、安全性評価の次の段階である定性的解析でおこなわれる。

移動ロボットにおける潜在危険制御系の構成事例からもわかるように、複雑な系では、全ての異常モードに対してフェイル・セーフ形解離を行う潜在危険制御系を構成する、すなわち「絶対安全なフェイル・セーフ・システム」とすることは、原理的に不可能である。従って、系の安全化を図るに際しては、潜在危険抑制原理(1),(2) による潜在危険抑制措置の検討も、総合的かつ効果的に実施していくことが必要である。この際、フェイル・セーフ事象といえども確率事象であり[76]、抑制手段の優先順位の決定などのために、残存リスクの確率論的評価、すなわち安全性評価過程(3),(4) の実施が重要となる。

潜在危険制御系に関する議論は、潜在危険、解離される作用鎖、解離に関する細目（解離原理、解離作用、その定量的制御方式など）、制御連鎖に関する細目（生じ得る変化、反転作用鎖の解離など）を特定して行われることが肝要であり、そのためには安全性評価の第１段階「潜在危険の同定」が系統的に行われていなければならない。その理由として、

（１）高度なロボットにより構成される複雑な系では、未知の現象も含めて、一般に生じ得るすべての変化および潜在危険を事前に容易には特定できない。

（２）一つの系内に相反潜在危険が生ずる場合、潜在危険制御系による制御の方向が逆になる。

３．６　結　　言

従来、フェイル・セーフ・システムなど潜在危険抑制措置に関する基本的な概念は、機械、電子、情報、化学などの異なる工学体系間で一般化されておらず、その整合性に欠ける面があった。ロボットなど、各種工学体系を包括する複雑な系の安全性向上を図る場合、潜在危険抑制措置の構成法が体系化され、またその構成のための系統的方法論が確立していることが必要である。

本章では、Ａ－Ｃモデルを拡張することにより、まず潜在危険抑制過程を：

（１）作用源の排除、（２）変化の抑制、（３）系の毀損生成相遷移の禁止、（４）系の毀損生成相からの遷移、の各潜在危険抑制原理として体系化した。

次に、潜在危険抑制原理（３）および（４）を実現する潜在危険抑制措置の構成法則を、潜在危険制御系による作用鎖の解離法則として一般化・体系化することにより、複雑な系における潜在危険の同定と潜在危険制御系の構成とを系統的に行うための方法論が確立された。

また、フェイル・セーフ・システムやフォールト・トレラント・システムの概念が異なる工学体系間に共通して適用できるように一般化され、潜在危険制御系の重要な下位要素である検出部、信号処理部、出力部などからなる情報処理系をフェイル・セーフ・システムとして構成可能とするための必要条件が明らかとなった。

さらに、自律移動ロボットの潜在危険制御系が本方法論に基づいて構成された。本章では、ロボットが静止対象物と衝突する潜在危険および移動対象物がロボットに衝突する潜在危険を同定し、まず潜在危険抑制原理（３）を適用した潜在危険制御系が構成された。次に、抑制原理（４）を適用して、それぞれ単純制動衝突回避、対スキッド制御制動衝突回避、平衡制御制動衝突回避、および経路制御単静止対象物衝突回避、経路制御多静止対象物同時衝突回避、動対象物衝突回避を実現する潜在危険制御系が構成された。そして、潜在危険制御系への可フェイル・セーフ情報処理系と可フォルト・トレラント情報処理系の適用範囲が明確化された。

第４章　災害発生機構の解析のための包括的論理モデル

４．１　緒　　言

前章までに、ロボットの潜在危険の同定と潜在危険制御系の構成について論じ、実際の系では、多様な故障モードが存在するので、潜在危険抑制手段の優先順位の決定や残存リスクの評価を行うために、定性的および定量的安全性解析を実施することが必要であることを述べた。

ＦＴＡ（Fault Tree Analysis ）は、定性的および定量的安全性解析を行うために開発された方法論である[77]。この方法論を用いて、同定された潜在危険による災害の発生機構を演繹的に解析することができる。

災害発生機構の解析は、通常、具体的に条件が与えられた個々の系を対象として行われる。一方、個々の系に実施された解析に見落としがないかなどをチェックする機能が非常に重要である。このような機能は、同定された潜在危険による災害の発生機構について、その想定し得るすべての場合を考慮した包括的論理モデル（以下単に論理モデルという）を展開しておくことによって得られる。このような目的で開発された論理モデルとして、ＭＯＲＴ（Management Oversight and Risk Tree ）があげられる[78]。しかし、ＭＯＲＴは、災害発生要因のうち特に安全管理上の見落としをチェックするための論理モデルであり、これをそのままハードウエア要因の比重が高い人間－ロボット系の災害発生機構の解析のための論理モデルとしては適用できない。

本章では、今後出現の予想される人間－ロボット系にも適用可能な論理モデルを展開する。また、次の段階の定量的解析に必要となる系の相分割について論じる。さらに、系の代表的な相における最小カット集合を求め、各相におい

て論理構造上重要となる潜在危険抑制措置について検討する。

4．2　論理モデルの記述方法と頂上事象

本研究では、論理モデルをFT(Fault Tree)[79] の記号を用いて記述する。

論理モデルの頂上事象は、ロボットの人間に対する潜在危険による災害の発生である。潜在危険と災害については、第2章において多様なものが同定されている。本章では、それらのうち、ロボットから人間への作用連鎖1形における運動エネルギ伝播形作用による災害として、「人がロボットにより打たれる災害」（図4-1、E：事象識別記号；以下同様とする）を取りあげる。

論理モデルの頂上事象「人がロボットにより打たれる災害」（図4-1、E）は、「ロボットの転倒」（Ea01）、「ロボットの墜落」（Ea02）、転倒や墜落以外に生ずる「ロボットの本体の運動」（Ea03）、「腕の運動」（Ea04）または「ロボットの扱い物の運動」（Ea05）によって打たれるものとに分類できる。本章では、さらに、ロボットの本体または腕によって打たれる災害発生の論理モデルを展開する。

4．3　ロボットの本体に打たれる事象生起の論理モデル

「ロボットの本体に打たれる」事象は「ロボット本体が運動する」（Eb07）、その運動エネルギから「防護の不適（ＬＴＡ）」（Eb08）、および「運動エネルギを受け得る危険域に人が存在する」（Eb09）事象全てが存在することにより生起し、「その運動の速度や出力」（Condition 1）を条件としてロボットの本体に打たれる災害（図4-1,Ea03）が発生する。

4．3．1　ロボット本体の運動（図4-1、Eb07）

この事象は、外力がロボットへ作用して生ずる「他律的運動」（Ec05）とロボット自体の動力源により生ずる「自律的運動」（Ec06）とに分類できる。

a．ロボット本体の他律的運動（図4-1、Ec05）

この事象は、「外力の作用」（Ed04）下で、ロボットあるいはその支援システムが、ロボットの力学的「安定化に失敗」（Ed03）することによって生ずる。ただし、安定化に失敗する各モードと外力の種類との可能な組合せは、「外力の強度に依存」（Condition 2）している。

a-i．ロボットの力学的安定化に失敗（図4-1、Ed03）

この事象が生起するモードには、ロボットの力学的安定化の「非自動制御時」（Ec04）と「自動制御時」（Ec05）とがある。

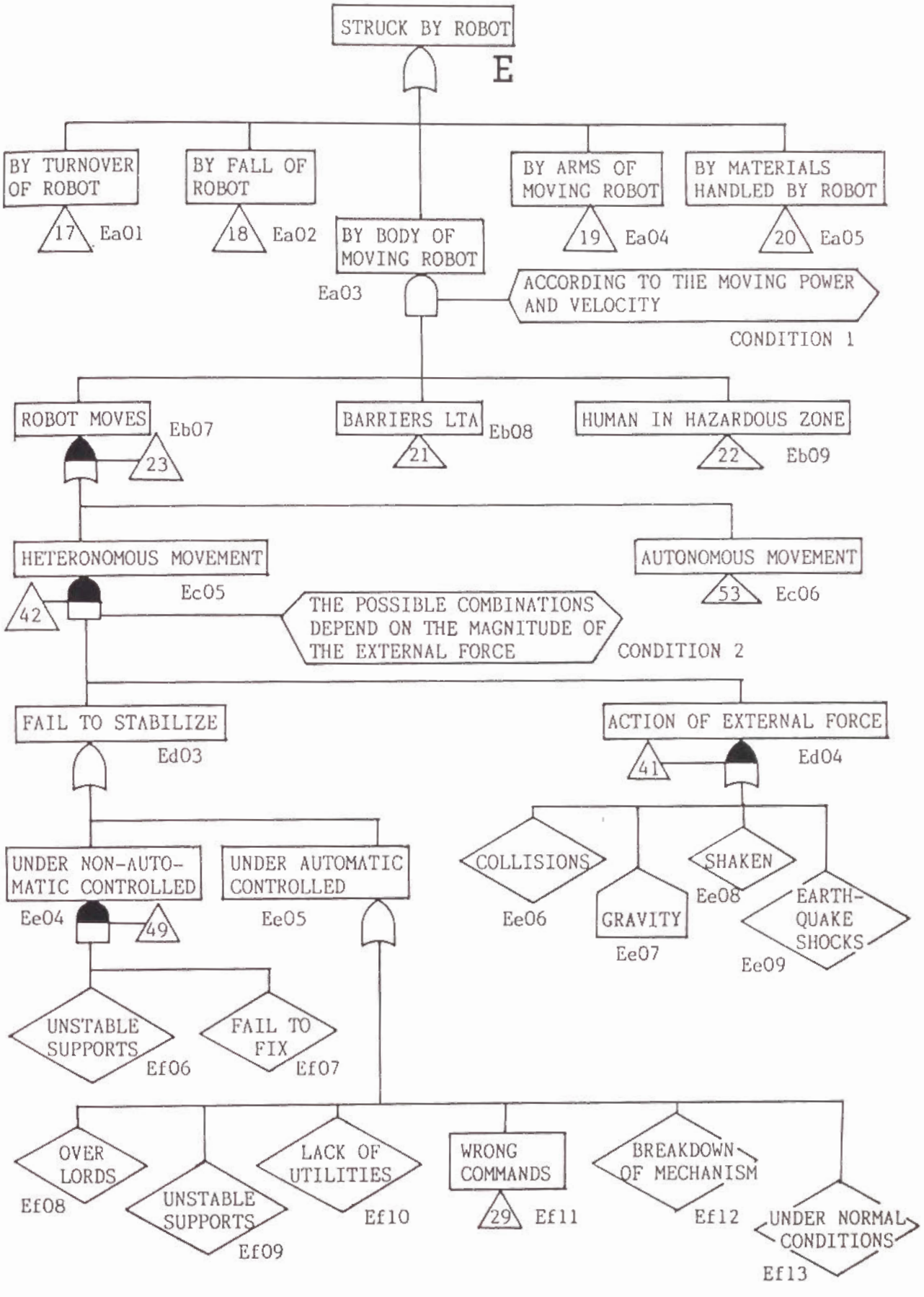
a-i-i．非自動制御時に安定化に失敗（図4-1、Ec04）

この事象は、ロボット支援システムの「不安定な支持」（Ef06）と、ロボットまたは支援システムが外力の作用時にロボットの「固定に失敗」（Ef07）することによって生ずる。

a-i-ii．自動制御時に安定化に失敗（図4-1、Ec05）

この事象は、ロボットへの「過負荷」（Ef08）、ロボットの支持機構の「不安定な支持」（Ef09）、ロボットへの動力や情報供給の「欠如」（Ef10）、制御系での「誤命令」（Ef11）の発生、装置の「故障」（Ef12）などの原因により生じ、外力の大きさによっては、「正常な制御時」（Ef13）にも発生し得る。このうち「誤命令」（Ef11）は、転出部位No.29（図4-4、事象 Ec17 下）の仕分けＯＲゲートへ連結される。

本論文では、論理形式として抽象化あるいは一般化されたゲート以下の部分ツリーが他のゲート以下に重複するのを避けるために、特殊な記号である「仕分けＡＮＤゲート」および「仕分けＯＲゲート」を用いる。これらのゲートからの出力は、入力の論理的表現は等価であっても、その具体的意味が異なるときには、ゲート上部および転出部位のうちから該当する部位のみを選んで発生するものとする。



LTA: Less Than Adequate

図４－１　ロボットによる災害を解析するための包括的論理モデル（その１）

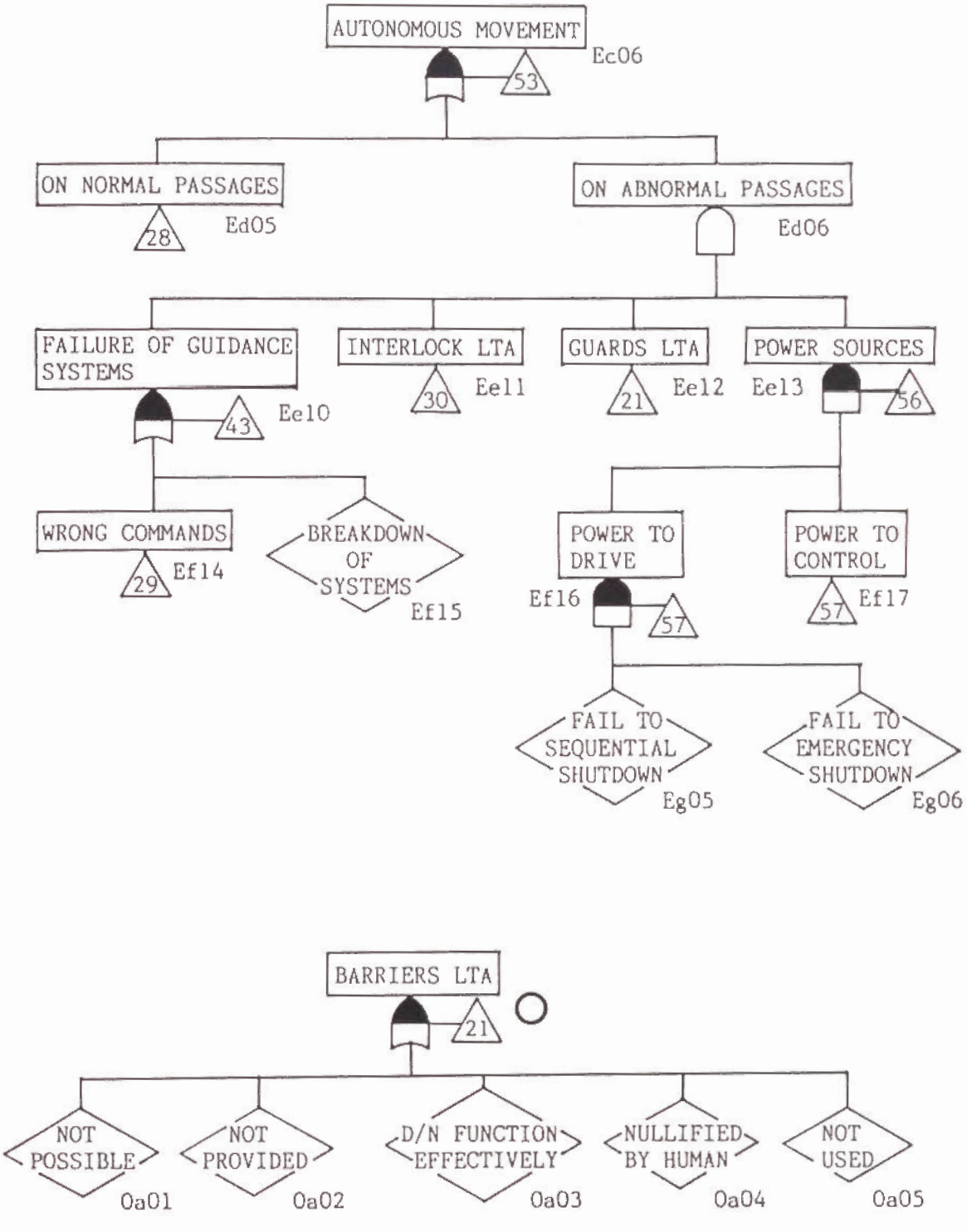


図４－２　ロボットによる災害を解析するための包括的論理モデル（その２）

a-ii．ロボットへの外力の作用（図4-1、Ed04）

この事象は、ロボットが何かに、あるいはロボットへ何かが「衝突」（Ee06）したり、地上での「重力」（Ee07）、「人為的な揺動」（Ee08）、「地震」（Ee09）によって生ずる。

b．ロボット本体の自律的運動（図4-1 および図4-2、Ec06）

この事象の発生モードには、ロボットの「正常な移動路」（図4-2、Ed05）で生ずるものと「異常な移動路」（図4-2、Ed06）で生ずるものとがある。

b-i．正常な移動路でのロボットの自律的運動（図4-2、Ed05）

これは、図4-4 （事象Ec08下の）転出部位No.28 へ連結される。

b-ii．異常な移動路でのロボットの自律的運動（図4-2、Ed06）

これは、「ロボットの誘導システムの失敗」（Ee10）、異常を検知して自発的に停止するための「インターロックの不適」（Ee11）、ロボットを強制的に停止させる「防護物の不適」（Ee12）、およびロボットを作動させる「動力源の存在」（Ee13）事象が全て生起することにより生ずる。このうち「インターロックの不適」事象は、図4-4 （事象Ed10下の）転出部位No.30 へ、「防護の不適」（Ee12）事象は、図４－２（事象Ｏ下の）転出部位No.21 へそれぞれ連結される。

b-ii-i．ロボットの誘導システムの失敗（図4-2、Ee10）

これは、制御系への「誤命令」（Ef14）の発生、または「誘導システムの故障」（Ef15）により生ずる。前者の事象Ef14は図4-4 （事象Ee17下の）転出部位No.29 へ連結される。

４．３．２　防護の不適（図4-1、Eb08）

ここでの防護とは、ロボット、ロボットと人との間、または人において、災害発生の直接原因となるエネルギの伝播を阻止または緩衝する機能を意味し、ロボットの制動機構、衝突緩衝装置、人体への保護具などで構成される。

事象Eb08は、図4-2 （事象Ｏ下の）転出部位No.21 へ連結される。この事象

の原因モーには、防護が技術的に「不可能」（図4-2、0a01）、可能であるがそれが「用意されていない」（0a02）、用意されているが故障や性能など機構自体の原因で「効果的に機能しない」（0a03）、設置されているものを「人が無効にする」（0a04）、そして保護具や安全装置など用意されていて取付けて使用すべきものを「使用しない」（0a05）がある。

4．3．3　危険域に人の存在（図4-1、Eb09）

この事象は、図4-5（事象N下の）転出部位No.22 へ連結される。

4．4　ロボットの腕に打たれる事象生起の論理モデル

「ロボットの腕に打たれる」事象は、論理モデル（図4-3 ）に展開されるように、ロボットの「腕の運動」（Eb10）、「防護の不適」（Eb11）および「危険域に人の存在」（Eb12）事象全てが存在することにより生起し、「運動の出力と速度」（Condition 3）を条件としてロボットの腕に打たれる災害（図4-1 および図4-3、Ea04）が発生する。

4．4．1　ロボットの腕の運動（図4-3、Eb10）

腕の運動モードとして、ロボット本体の運動とは独立してしかも外力が作用することによる「他律的運動」（Ec07）、腕の動力源による「自律的運動」（Ec08）、または「ロボット本体に連動した運動」（Ec09）がある。

a．腕の他律的運動（図4-3、Ec07）

この事象は、腕に「外力が作用」（Ed08）するとき、腕の力学的「安定化に失敗」（Ed07）することにより生ずる。ただし、安定化に失敗する各モードと外力の可能な組合せは、外力の大きさに依存している（Condition 4）。

a-i．腕の力学的安定化に失敗（図4-3、Ed07）

これは、腕の運動の「非自動制御下」（Ee14）に生ずる場合と「自動制御下」（Ee15）に生ずる場合とがある。

a-i-i．非自動制御下で力学的安定に失敗（図4-3、Ee14）

これは、図4-1（事象Ee04下の）転出部位No.49へ連結される。

a-i-ii．自動制御下で力学的安定化に失敗（図4-3、Ee15）

これは、「装置の故障」（Ef18）、「過負荷」（Ef19）、動力源や情報など必要物の「欠如」（Ef20）、制御系への「誤命令の発生」（Ef21）、そして外力の大きさによっては「正常な制御状態」（Ef22）によっても生ずる。このうち、事象Ef21は、図4-4（事象Ee17下の）転出部位No.29へ連結される。

a-ii．腕に外力が作用する（図4-3、Ed08）

この事象は、図4-1（事象Ed04下の）転出部位No.41へ連結される。

b．自律的運動（図4-3、図4-4、Ec08）

この事象は、制御系への「動作命令」（Ed09）、人の存在などの異常を検知してロボットを運動状態へと移行させないための「インターロッキングの失敗」（Ed10）、および運動のための「動力源の存在」（Ed11）事象がすべて生起することにより生ずる。

b-i．動作命令（図4-4、Ed09）

動作命令は、ロボットの管理上から「意図された命令」（Ee16）と「意図されない命令」（Ee17）とに分類できる。

b-i-i．意図された動作命令（図4-4、Ee16）

これは、ロボットの作動「プログラムの開始」（Ef23）や「一時的停止条件の解消」（Ef24）などにより生ずる。

b-i-ii．意図されない動作命令（図4-4、Ee17）

これは、「制御の失敗」（Ef25）、「プログラムの不適」（Ef26）、「プログラム選定の誤り」（Ef27）、またはその他の「人的操作の誤り」（Ef28）により生ずる。

（i）制御の失敗（図4-4、Ef25）

この事象は、「サーボ機構の異常」（Eg07）、「電子回路の異常」（Eg08）、制御系への「誤信号の発生」（Eg09）または「その他の部分の異常」（Eg10）によって生ずる。

（i-i）サーボ機構の異常（図4-4、Eg07）

これは、油圧系の「油の汚濁」（Eh01）、「サーボ弁の故障または異常」（Eh02）あるいは「油空圧など制御系への必要物供給の欠如」（Eh03）などにより生ずる。

（i-ii） 電子回路の異常（図4-4、Eg08）

これは、回路の「断線」（Eh04）、「短路」（Eh05）、「電子部品の劣化」（Eh06）などにより生ずる。

（i-iii）誤信号の発生（図4-4、Eg09）

これは、「静電気放電」（Eh07）、「瞬間停電」（Eh08）、「内部発生源からのノイズ」（Eh09）、「外部発生源からのノイズ」（Eh10）、「内界センサの異常」（Eh11）、「外界センサの異常」（Eh12）、「関連する装置からの誤信号」（Eh13）または「プログラム読み取りエラー」（Eh14）などにより生ずる。

b-ii．インターロックに失敗（図4-4、Ed10）

この事象は、装置が人の存在などの「異常の検知に失敗」（Ee18）、「作動に失敗」（Ec19）、人がインターロック装置を「無効にする」（Ee20）、またはインターロック機構が「設置されていない」（Ee21）などにより生ずる。

4．4．2　防護の不適（図4-3、Eb11）

事象Eb11は、図4-2（事象O下の）転出部位No.21 へ連結される。

4．4．3　危険域に人の存在（図4-3、Eb12；図4-5、N）

事象Eb12は、図4-5（事象N下の）転出部位No.22 へ連結される。

「危険域に人が存在」（図4-5, N）事象は、人がそこへ「必要上接近して」（Na01）生ずるものと「不必要に接近して」（Na02）生ずるものとがある。

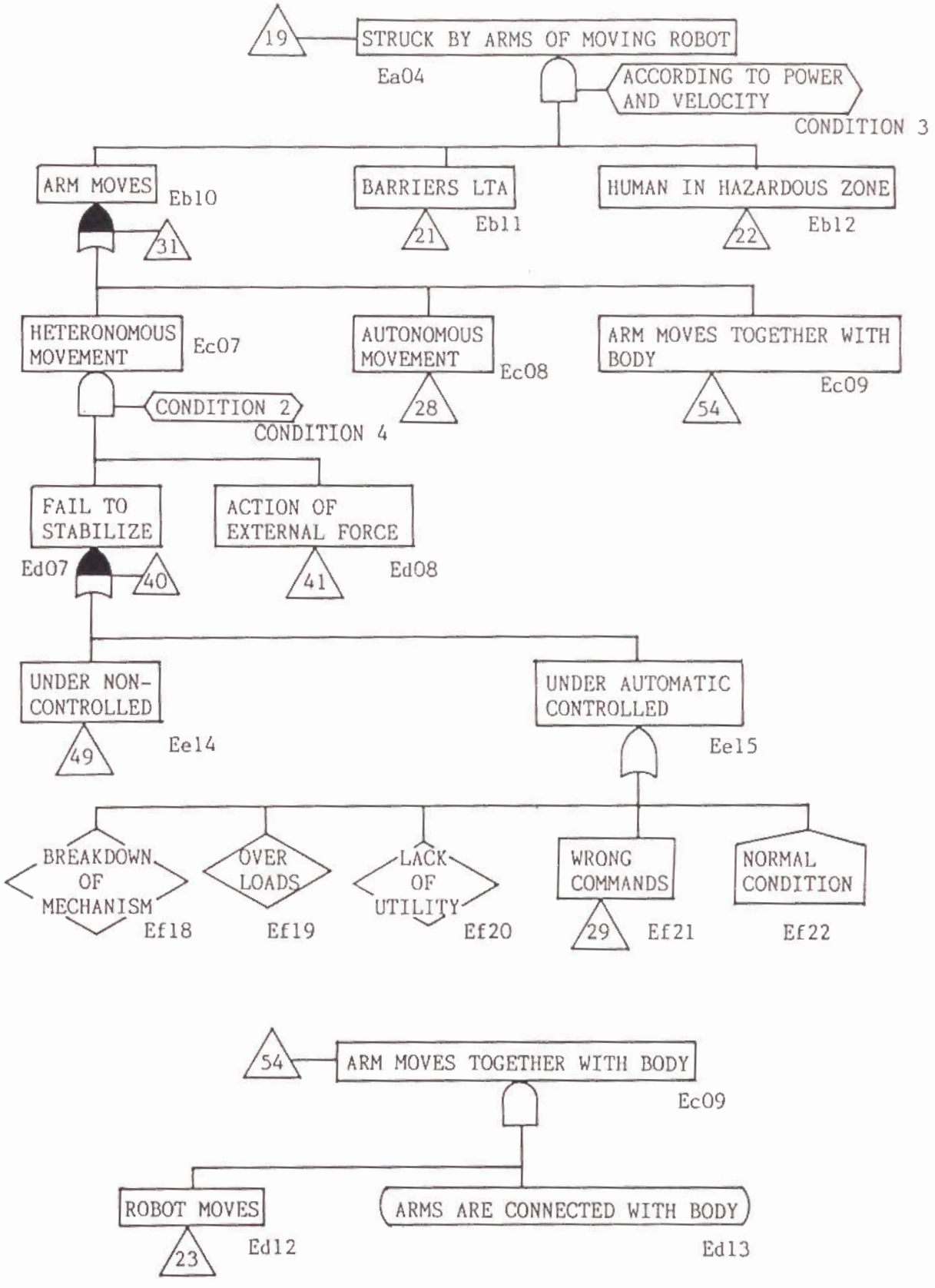


図４－３　ロボットによる災害を解析するための包括的論理モデル（その３）

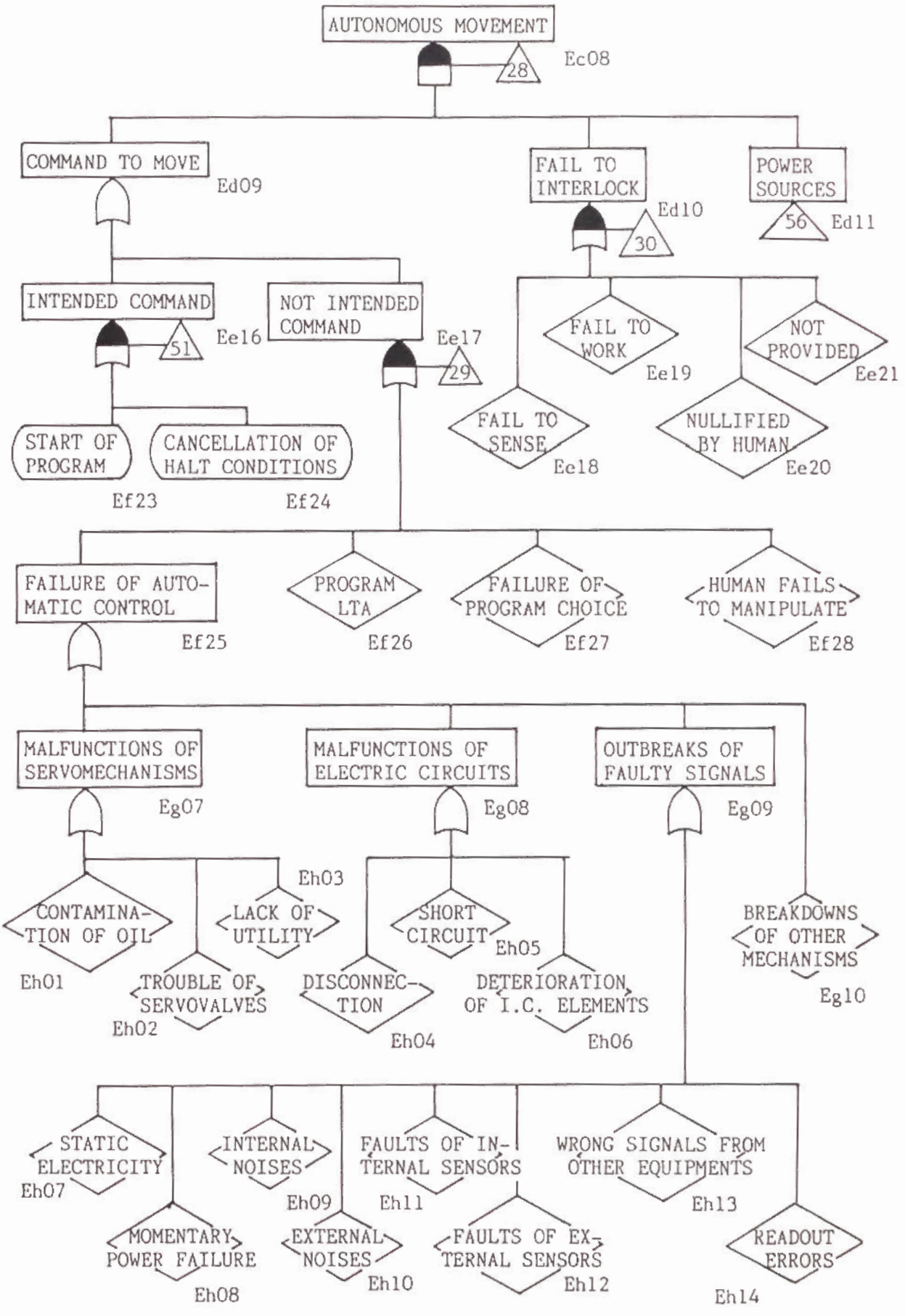


図４－４　ロボットによる災害を解析するための包括的論理モデル（その４）

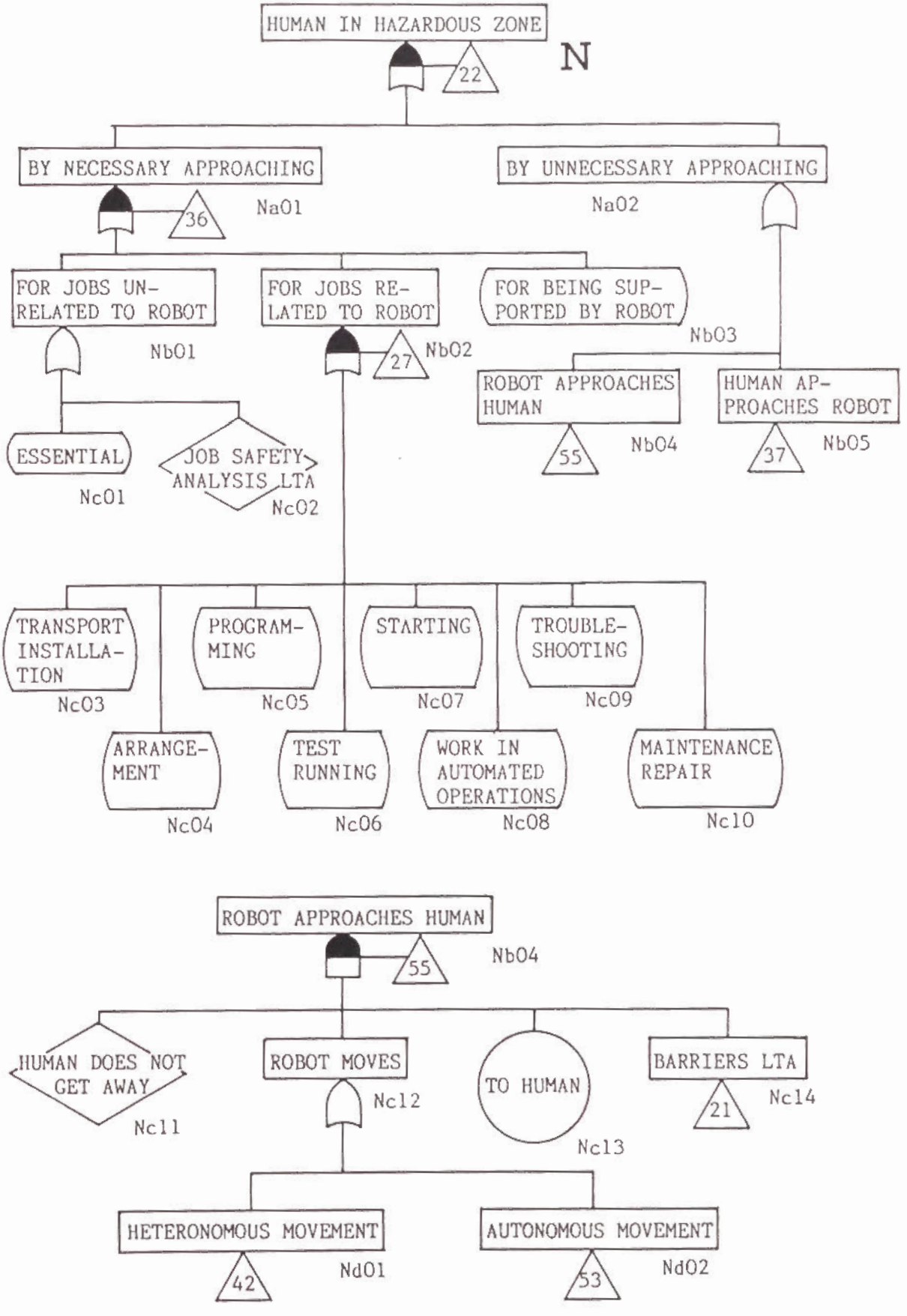


図４－５　ロボットによる災害を解析するための包括的論理モデル（その５）

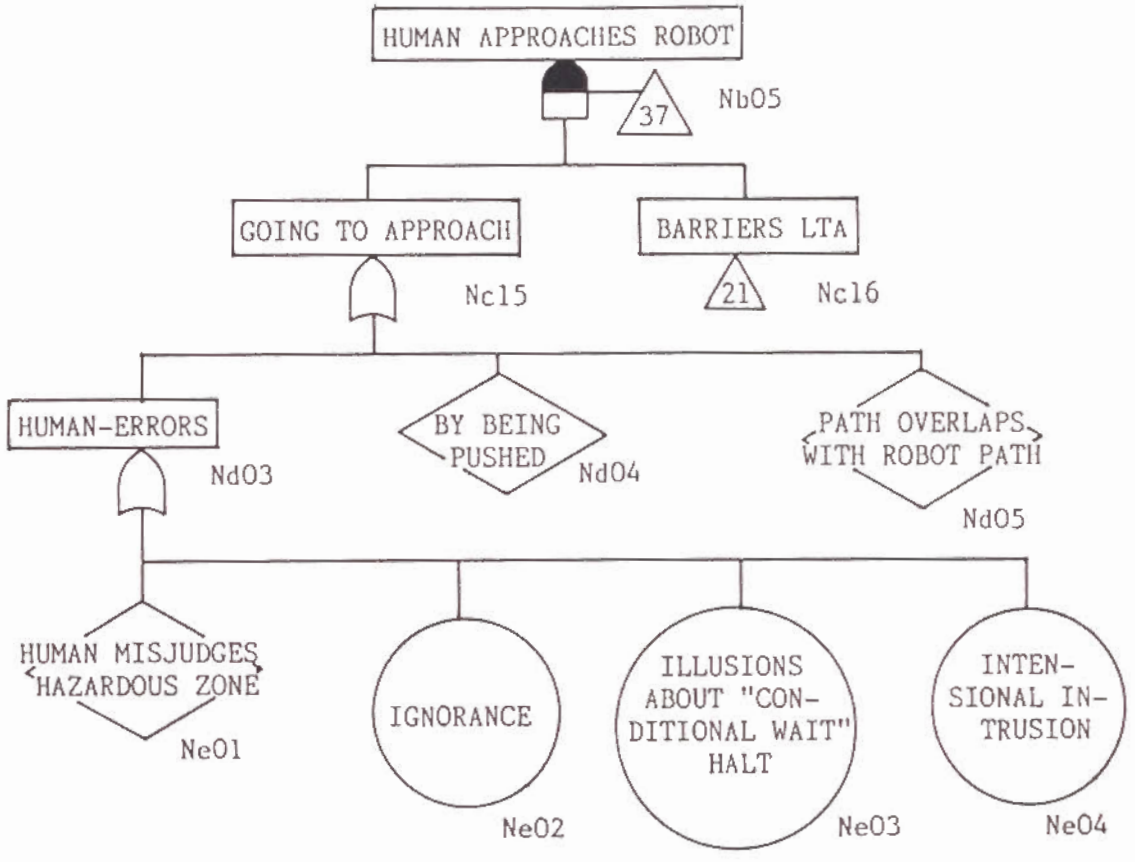


図４－６　ロボットによる災害を解析するための包括的論理モデル（その６）

表４－１　　仕分けゲート位置一覧

転出番号	仕分けゲート上の事象識別記号	
２１	O	（図４－２）
２２	N	（図４－５）
２３	Eb07	（図４－１）
２７	Nb02	（図４－５）
２８	Ec08	（図４－４）
２９	Ee17	（図４－４）
３０	Ed10	（図４－４）
３１	Eb10	（図４－３）
３６	Na01	（図４－５）
３７	Nb05	（図４－６）
４０	Ed07	（図４－３）
４１	Ed04	（図４－１）
４２	Ec05	（図４－１）
４３	Ee10	（図４－２）
４９	Ee04	（図４－１）
５１	Ee16	（図４－４）
５３	Ec06	（図４－２）
５５	Nb04	（図４－５）
５６	Ee13	（図４－２）
５７	Ef16	（図４－２）

a．必要上接近して存在（図4-5,Na01）

この事象は、「ロボットに無関係の業務」（Nb01）、「ロボットに関係した業務」（Na02）または「ロボットによる補助機能を受ける」（Eb03）ために生ずる。

a-i．ロボットに無関係の業務で存在（図4-5,Nb01）

これは、「本質的に不可避」（Nc01）な場合や、避け得るにもかかわらず「作業安全解析の不適」（Nc02）に代表される安全管理上の見落としにより生ずる。

a-ii.ロボットに関連した業務で存在（図4-5,Nb02）

これは、ロボットの「運搬・設置作業」（Nc03）、「段取り・調整作業」（Nc04）、「教示作業」（Nc05）、「ためし運転」（Nc06）、「起動操作」（Nc07），「自動運転付随作業」（Nc08）、「異常処理作業」（Nc09）、または「保全・修理作業」（Nc10）により生ずる。

b．不必要に接近して存在（図4-5,Na02）

この事象は、「ロボットが人間に不必要に接近する」（Nb04）ことによるものや、「人が不必要に危険域に入りこむ」（Nb05）ことにより生ずる。

b-i．ロボットが人に接近する（図4-5,Nb04）

この事象は、ロボットが「人の方向へ」（Nc13）、「移動」（Nc12）したとき、「人が逃げず」（Nc11）、「防護の不適」（Nc14）の全事象が存在することにより生起する。

b-i-i．移動（図4-5,Nc12）

ロボットの「移動」（Nc12）には「他律的運動」（Nd01）によるものと「自律的運動」（Nd02）によるものがあり、それぞれ図4-1（事象Ec05下の）転出部位No.42 および図4-2（事象Ec06下の）転出部位No.53 へ連結される。

b-i-ii.防護の不適（図4-5,Nc14）

事象Nc14 は、図4-2（事象O下の）転出部位No.21 へ連結される。

b-ii．人がロボットに近づく（図4-5,図4-6,Nb05）

この事象は、人がそこに「入ろうとする」（Nc15）事象と、柵や表示などによりそれを防ぐ「防護の不適」（Nc16）事象がともに生起することにより生ずる。

b-ii-i．人が入ろうとする（図4-6、Nc15）

この事象は、「人的過誤」（Nd03）、周囲の機械や装置に押されるなどの「影響によって」（Nd04）、または「人の通路がロボットの移動路と重なっている」（Nd05）などにより生ずる。

（i）人的過誤（図4-6、Nd03）

この事象は、「人が危険域の判断を誤って入ろうとする」（Ne01）、「危険域について全く知らないで入ろうとする」（Ne02）、「ロボットの条件待ち停止を完全停止と錯覚して入ろうとする」（Ne03）、または「危険を承知で故意に侵入しようとする」（Ne04）により生ずる。

b-ii-ii．防護の不適（図4-6、Nc16）

これは、図4-2（事象O下の）転出部位No.21へ連結される。

以上の論理モデル（図4-1～図4-6）における転出部位すなわち仕分けゲートの位置を、転出番号に対して仕分けゲート上の事象識別を対応させることにより、一覧表として表4-1に示す。これにより転入部位から転出部位を容易に見いだすことが可能である。

4．5　系の相分割と最小カットセット

ＦＴＡでは、頂上事象の発生確率を求めるなどして安全性の定量的評価を行う。このとき、ＦＴを構成する基本事象間の生起に関して統計的独立性が仮定できない場合は、定量化が極めて複雑になる。

論理モデルでは、例えば「ロボットに関連した作業」（Nb02）以下の各事象と「安定化に失敗」（Ed03）以下の各事象の生起が相互に依存するように、一般的条件下での系の基本事象の生起に関して統計的独立性は期待できない。

この問題に対処する手段として、系の相分割が考えられる。ここで系の相分

割とは：1．論理モデルを検討して、系の基本事象間の相互依存性に支配的な特性を探索する、2．それらの特性を適当なモードに分割する、3．各特性のモードを結合することにより得られる系のある局面では、基本事象間の統計的独立性が期待できるようにする；ものである。

人間－ロボット系では、これまで検討してきた論理モデルから：（1）ロボットの運転および修理などの状態、（2）ロボットの自律的または他律的運動形態、（3）人の存在形態；を表す特性をモード分割して、系の相分割を行うことが考えられる。

系全体の定量的評価は、系の各相で得られる定量的評価の結果を統合することにより比較的容易に得ることができよう。

4．5．1　系の特性とそのモード分割

系の特性を次ぎのようにモード分割する：

（1）ロボットの運転や修理などの特性モード；(i) 運搬・設置、(ii)段取り・調整、(iii) 教示、(iv)ためし運転、(v) 起動、(vi)自動運転、(vii) 保全・修理モード。

（2）ロボットの運動特性モード；(i) 意図された命令による自律的運動、(ii)意図されない命令による自律的運動、(iii) 他律的運動モード。

（3）人の存在特性モード；(i) 必要上接近して存在、(ii)不必要に接近して存在するモード。

4．5．2　特性モードとそれらの結合性

各特性モード間の結合性を考察する。

（1）運搬・設置モードや段取り・調整モードでは、ロボットが自動制御下にない場合が多く、他律的運動モードとの結合性が強い。

（2）教示、ためし運転、あるいは起動モードでは、接近している作業者がロボットの正常動作を把握している場合が多く、相対的に意図されない命令による自律的運動モードとの結合性が強い。

（３）自動運転モードでは、意図されたあるいは意図されない命令による自律的運動モードとの結合性が強い。

（４）保全・修理モードでは、そのときの状況によって、どちらの運動モードとも結合性が強まる。

（５）人が必要上接近して存在するモードでは、そのときの状況によって、どの運動モードとも結合性が強まる。

（６）人が不必要に接近して存在するモードでは、意図された命令による自律的運動モードとの結合性が強くなる。これは、ロボットの動作を把握していない人間が不必要に接近する場合が多いためである。

以上の検討結果を図4-7 として纏める。

４．５．３　系の代表的な相における主な最小カット集合

系の相を、記号「（状態特性モード(i～vii)――運動特性モード(i～iii)――存在特性モード(i～ii)）」で表すものとする。

系の代表的な相：(i-iii-i),(ii-iii-i),(iii-ii-i),(iv-ii-i),(v-ii-i),(vi-i-i),(vi-i-ii),(vi-ii-i),(vii-ii-i),(vii-iii-i)；において求められる主要な最小カット集合を表4-2 に示す。

ここでは、仕分けゲートからの出力は一箇所のみに発生し、基本事象が互いに独立であると仮定している。以上の前提条件から、各カットは、その具体的内容によって、事象Ea03または事象Ea04のいずれかを発生することになる。

最小カット集合を構成する基本事象は、より多くのカットに含まれるもの程ＦＴ構成上の構造的な重要度がより高いという定性的性質を持つ。そこで、定性的には、構造的な重要度の高いＦＴ構成事象程、より優先度の高い抑制措置の検討対象となる。以下に、系の代表的な相における主要な最小カット集合を考慮することにより、全カット集合に共通して重要な防護措置以外で重要となる潜在危険抑制措置を検討する。

（１）系の相(i-iii-i) および(ii-iii-i)では、事象Ef06およびEf07が構造的に重要である。これから、ロボットの運搬・設置・調整作業におけるロボット

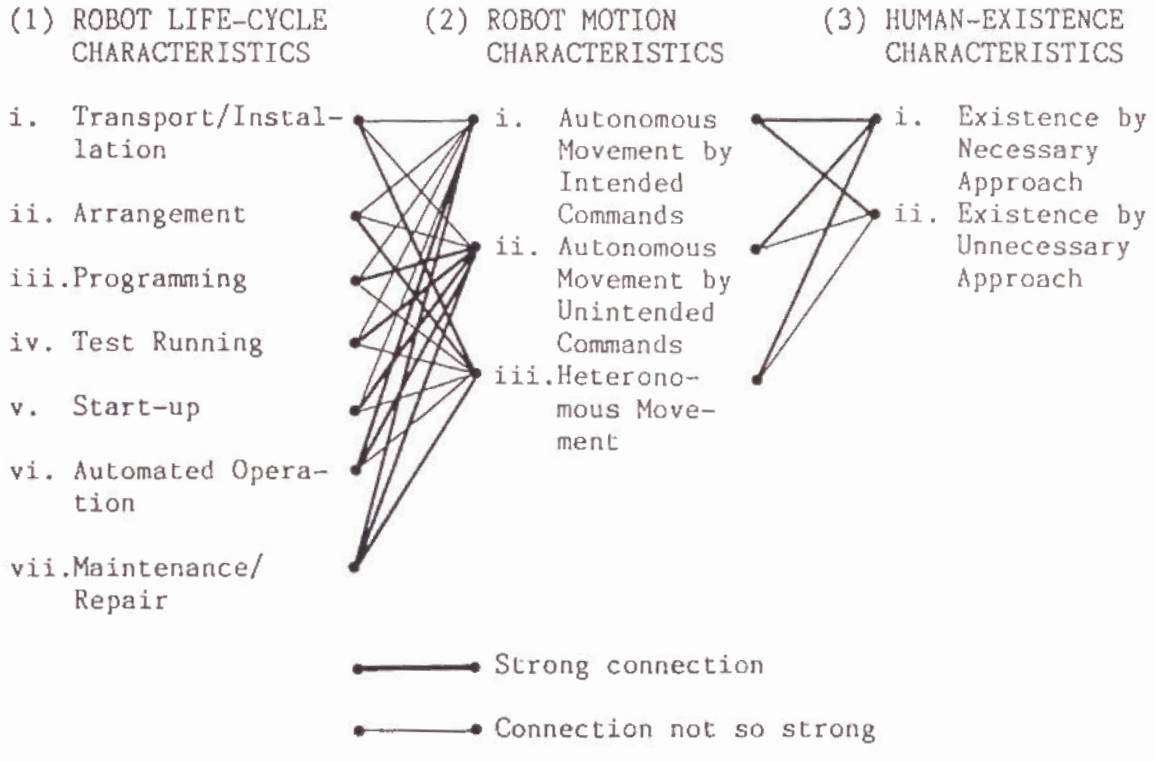


図４－７　系の相を構成するモードとその結合性

表４－２　論理モデルの主要な相における主な最小カット集合

系の相	Eb08（またはEb11）生起の条件下でEa03（またはEa04）を生起させる主な最小カット集合
i-iii-i	(Nc03, Ef06, Ef07, Ee07), (Nb03, Ef06, Ef07, Ee08) (Nb03, Ef06, Ef07, Ee06), (Nb09, Ef06, Ef07, Ee09) (Nb01, Ef06, Ef07, Ee07), (Nb01, Ef06, Ef07, Ee08) (Nb01, Ef06, Ef07, Ee06), (Nb01, Ef06, Ef07, Ee09)
ii-iii-i	(Nc04, Ef06, Ef07, Ee07), (Nb04, Ef06, Ef07, Ec08) (Nc04, Ef06, Ef07, Ee06), (Nc04, Ef06, Ef07, Ee09)
iii-ii-i	(Nc05, Ef23, Ed10, Ed11), (Nc05, Ef24, Ed10, Ed11) (Nc05, Ef25, Ed10, Ed11), (Nc05, Ef26, Ed10, Ed11)
iv-ii-i	(Nc06, Ef23, Ed10, Ed11), (Nc06, Ef24, Ed10, Ed11) (Nc06, Ef25, Ed10, Ed11), (Nc06, Ef26, Ed10, Ed11)
v-ii-i	(Nc07, Ef23, Ed10, Ed11), (Nc07, Ef24, Ed10, Ed11) (Nc07, Ef25, Ed10, Ed11), (Nc07, Ef26, Ed10, Ed11)
vi-i-i	(Nb01, Ee16, Ed10, Ed11), (Nc08, Ee16, Ed10, Ed11) (Nc09, Ee16, Ed10, Ed11), (Nb03, Ee16, Ed10, Ed11)
vi-i-ii	(Nc15, Nc16, Ee16, Ed10, Ed11) (Nc11, Nc12, Nc13, Nc14, Ee16, Ed10, Ed11)
vi-ii-i	(Nb01, Ef23, Ed10, Ed11), (Nb01, Ef24, Ed10, Ed11) (Nb01, Ef25, Ed10, Ed11), (Nb01, Ef26, Ed10, Ed11) (Nc08, Ef23, Ed10, Ed11), (Nc08, Ef24, Ed10, Ed11) (Nc08, Ef25, Ed10, Ed11), (Nc08, Ef26, Ed10, Ed11) (Nc09, Ef23, Ed10, Ed11), (Nc09, Ef24, Ed10, Ed11) (Nc09, Ef25, Ed10, Ed11), (Nc09, Ef26, Ed10, Ed11) (Nb03, Ef23, Ed10, Ed11), (Nb03, Ef24, Ed10, Ed11) (Nb03, Ef25, Ed10, Ed11), (Nb03, Ef26, Ed10, Ed11)
vii-ii-i	(Nc10, Ef23, Ed10, Ed11), (Nc10, Ef24, Ed10, Ed11) (Nc10, Ef25, Ed10, Ed11), (Nc10, Ef26, Ed10, Ed11)
vii-iii-i	(Nc10, Ef06, Ef07, Ee07), (Nc10, Ef06, Ef07, Ee08) (Nc10, Ef06, Ef07, Ec06), (Nc10, Ef06, Ef07, Ee09)

の他律的運動による潜在危険を抑制するには、ロボットの支持または固定を完全に行う措置が基本的に重要である。

（２）系の相(iii-ii-i),(iv-ii-i),(v-ii-i) および(vii-ii-i)では、人が作業のために危険域に入らなければならない条件下で、事象Ed10およびEd11が構造的に重要となる。これから、ロボットに接近して行う教示・ためし運転・起動・保全作業におけるロボットの自律的運動による潜在危険を抑制するには、ロボットの駆動エネルギの遮断や制限または人の存在に対するロボットの動作インターロッキングによる抑制措置が基本的に重要である。

（３）系の相(vi-i-i)および(vi-i-ii) では、事象Ec16,Ed10 およびEd11が構造的に重要であるが、自動運転モードであるので、事象Ec16およびEd11は常起事象である。従って、この相では、人の存在に対するロボットの動作インターロッキングが基本的に重要な抑制措置となる。

（４）系の相(vi-ii-i) では、事象Ed10およびEd11が構造的に重要であるが、自動運転モードであるので、前項(3) と同様に、ロボットの動作インターロッキングが基本的に重要な対策となる。

（５）系の相(vii-iii-i) では、人が作業のためにロボットに接近する条件下で、事象Ef06およびEf07が構造的に重要であり、保全作業におけるロボットの他律的運動による潜在危険を抑制するには、ロボットの支持または固定を完全に行う措置が構造的に重要となる。

４．６　結　　言

本章では、人間－ロボット系において、ロボットから人間への作用連鎖１形における運動エネルギ伝播作用により、人がロボットの本体または腕に打たれる災害発生の包括的論理モデルを展開した。このモデルにより、任意の具体的な人間－ロボット系において実施されたそれらの災害に関する定性的安全性解析に見落としがないかチェックすることができる。また、個々の系のＦＴは、この論理モデルを系の諸条件に従って特殊化することによっても得られる。

確率論などを用いた系の定量的評価を行う際には、基本事象間に統計的独立性が仮定できることが重要であり、そのための手段として系の相分割を行うことの必要性を述べ、相分割の方法を示した。さらに、系の代表的な相について、主要な最小カット集合を求めた。これに基づいて、それ等カット集合を構成する各事象のＦＴ構成上の構造的な重要度を考慮することにより、系の各相において重要となる潜在危険抑制措置を考察した。

第５章　順序依存形故障論理の定量化

５．１　緒　　言

前章では、第２章において同定された潜在危険により発生する災害のうち、人間がロボットの本体または腕によって打たれる災害を取りあげ、その発生機構を解析するための論理モデルを展開した。安全性の定量的評価は、このような論理モデルを具体的な系の諸条件に従って特殊化し、その結果として得られるＦＴを定量化することにより可能となる。

ＦＴの定量的解析アルゴリズムには種々のものが提案されており、原子力あるいは化学プラントなどへの実際的適用事例も多い[80-85]。人間－ロボット系の定量的評価に際してもそれらのアルゴリズムを適用することができよう。

本章では、人間－ロボット系のＦＴＡにおいては、入力事象の発生順序が出力事象の生起に本質的意味をもついわゆる順序依存形故障論理の定量化が必要となることを事例をあげて示す。そして、順序依存形故障論理での出力事象の生起確率および期待発生頻度を求めるためのアルゴリズムを提案する。

５．２　順序依存形故障論理の必要性

本章では、特に、事象の生起に関する表現として、「生起」を事象の生じている状態、「非生起」を生じていない状態、「発生」を事象が非生起から生起へ移行する状態変化、そして「修復」を事象が生起から非生起へ移行する状態変化の意味で用いる。

ＦＴで表現された論理モデルは、すべての最小カット構造をＯＲ結合したものと等価である[86]。ここに、最小カット構造とは、ひとつの最小カット集合を構成する入力事象（基本事象）A_1、A_2、…、A_nのＡＮＤ結合である。特に最小カット構造の出力事象Ｂの生起が、入力事象の発生順序に依存する場

合、その図式表現として図５－１に示すような優先ＡＮＤゲートが用いられる。

ここで、出力事象Ｂは、入力事象A_i（$i \in 1、2、\cdots、n$）が、A_1、A_2、…、A_nの順序、すなわち、図中、左から右への順序で発生し、そのおのおのが生起しつづけ、結果的にすべての入力事象が生起しているときにのみ生起するものと定義される。

この論理ゲートの具体的な必要例およびその定量化アルゴリズムに関しては、入力事象が非修理系（一度発生すると生起しつづける、すなわち入力事象が修復のない系）である場合に限って、文献83）において、主電源供給機と予備電源供給機からなる非修理系の電力供給系を例として論じられている。しかし、入力事象を修理系とした一般的な場合については、その必要例が、例えば文献87）に述べられているほかには見あたらない。

そこで、まず最小カット集合（以下単にカットと言う）の入力事象が修理系で順序依存形故障論理を必要とする事例を、入間－ロボット系の論理モデルから示す。

５．２．１　論理モデルから得られる系の代表的カット

前章において作成された論理モデルより、入がロボットの腕によって打たれるという事象を生起させるカットＣ（ｘ）として

$$C(x) = \{Eb11、Ee16、Ee18、Ed11、Nb05\} \tag{5-1}$$

を得る。

ここに

Eb11：ロボットの腕の運動エネルギが入へ伝播するのを阻止または緩衝する制動装置や緩動装置などの防護機能の不適

Ee16：ロボットの腕の動作制御系への意図された動作命令の生起

Ee18：入の危険域内への侵入など異常を検知して、腕が動作しないようにするインターロッキング機構における異常検出機構の故障

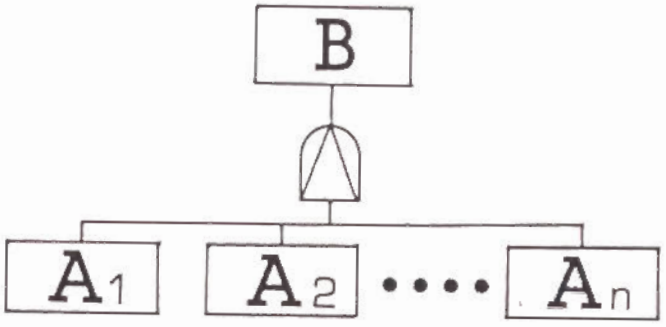


図５－１　発生順序依存形故障論理の図式表現

表５－１　入力事象の発生順序と出力事象との関係

ケース番号	入力事象			出力事象
	A_1	A_2	A_3	B
1	Ee16	Ee18	Nb05	生　起
2	Ee16	Nb05	Ee18	非生起
3	Ee18	Ee16	Nb05	生　起
4	Ee18	Nb05	Ee16	生　起
5	Nb05	Ee16	Ee18	非生起
6	Nb05	Ee18	Ee16	非生起

Ed11：腕を動作させる動力源の存在

Nb05：人の危険域内への侵入

である。

5．2．2　系の条件と入力事象の特性

系の条件を以下のように設定しても不自然ではない：

（1）「意図された動作命令」（Ee16）事象は、制御プログラムとロボット外部の作業状況などに従って、時間に対して不規則に生起または非生起をくりかえす。

（2）「異常検出機構の故障」（Ee18）事象は、異常検出センサの故障により生じ、故障センサは修理により正常状態へ復帰する。

（3）人はまれに危険域へ侵入し（Nb05）、ある短時間だけそこに留まる。

（4）防護機能は故障中である、すなわち事象Ed11は常に生起している。

（5）ロボットの腕の動力源（Ed11）は常に存在している。

（6）インターロッキングは、人の危険域への侵入を瞬時に検知して作動し、いったん作動すると、その後の異常検出機構の状態にかかわらず、人が危険域外へ退出して再起動操作をするまで解除されない。

5．2．3　入力事象の発生順序と出力事象の生起との関係

前節によって与えられた条件（4）および（5）より、カットC（x）は

$$C(x) = \{Ee16, Ee18, Nb05\} \qquad (5\text{-}2)$$

と縮小される。

ここで、カットを構成する入力事象Ee16、Ee18およびNb05は前節条件（1）、（2）そして（3）より、いずれも生起・非生起を無秩序にくり返し行うので、いわゆる修復のある入力事象となる。

ところで、式(5-2)によって定義されるカットが成立するためには、カット

を構成する事象すべてが生起していなければならないが、これは必要条件であって十分条件ではない。なぜならば、条件（６）によって、事象Nb05の発生よりも後で事象Ee18が発生した場合、Nb05の生起とともに作動したインターロッキングは事象Ee18の発生にもかかわらず機能し続けるからである。

したがって、このカットが成立するためには「異常検出機構の故障」（Ee18）が「人の侵入」（Nb05）に先だって生起していることが必要である。すなわち、カットを構成する事象が同時に発生する場合を確率論的に無視すれば[89]、事象の発生順序の取り得る組合せは６通りあるが、そのうちカットを成立させるものは、表５－１に示すように、ケース番号1,3,4 の３通りの場合に限られる。ここに、記号A_1, A_2, A_3 およびＢが、図５－１の最小カット構造（ｎ＝３）の各事象に該当する。

インターロッキング機構を有する人間－ロボット系において、ロボットの自動運転モードでの論理モデルからの主要なカットは、ほとんどの場合インターロッキングの異常に関する人力事象を含む（表４－２参照）。インターロッキングが前節条件（６）のような機構であるとき、人間－ロボット系のＦＴＡにおいては修理系での順序依存形故障論理を考慮しなければならない場合が多い。

一般的に、自動化された機械を含む人間－機械系においては、修理系での順序依存形故障論理の必要性が高いといえる。

５．３　順序依存形故障論理の定量化アルゴリズム

修復系入力事象からなる順序依存形故障論理の定量化に関しては、入力事象が定数発生率と修復率をもつ指数分布に従う場合、原理的にはMarkovモデルが適用できる[90]。

カットを構成する入力事象の生起に関して、その相互の統計的独立性が仮定できるとき、修復系人力事象からなる順序依存形故障論理は、Markovモデルを用いずに、以下に示す簡便なアルゴリズムによって定量化される。

5．3．1　記号の定義

本論文で用いる基本的な記号を以下のように定義する：

n　：優先ＡＮＤゲートへの入力事象の数

x　：ｎ個の異なる入力事象1,2,･･･,n が事象x_1，x_2，・・・，x_n の順序で発生し、結果的に全入力事象が同時に生起することを表す入力事象の発生順序ベクトル［x_1，x_2，・・・，x_n］

X　：ｎ！個存在する発生順序ベクトルｘの集合

X_1：優先ＡＮＤゲートの出力事象を生起させる発生順序ベクトルｘの集合

λ_{x_i}：入力事象x_iの時刻ｔでの非生起の条件下での単位時間あたりの発生確率

μ_{x_i}：入力事象x_iの時刻ｔでの生起の条件下での単位時間あたりの修復確率

$G_{x_i}(t-\tau_i)$：入力事象x_i の時刻τ_i での発生による生起が時間ｔまでに修復されている確率

$Q_{x_i}(t)$：入力事象x_i が時刻ｔで生起している確率

$w_{x_i}(t)$：入力事象x_iの時刻ｔでの単位時間あたりの発生回数の期待値

$Q^*(t)$：出力事象が時刻ｔで生起している確率

$w^*(t)$：出力事象の時刻ｔでの単位時間あたりの発生回数の期待値

$W^*(0,t)$：出力事象の時刻0からｔまでの発生回数の期待値

L^{-1}：ラプラス逆変換作用素

s　：ラプラス変換変数

t，τ_i，μ_i：時間およびそのパラメータ

$(t,\ t+\alpha]$：時刻ｔからｔ＋αまで（ｔは含まず、ｔ＋αは含む）。

5．3．2　アルゴリズム

カットを構成するｎ個の入力事象に対して、次の仮定をおく。

（１）各入力事象1,2,･･･,n は、その生起に関して相互に統計的に独立である。

（２）各入力事象は、定数発生率λ_iと修復率μ_i（i=1,2,･･･n）をもつ指数分布でモデル化され、ｔ＝０では各々非生起である。

（３）各入力事象が、任意の微小時間$(t, t+\Delta t]$で２回以上発生する確率は、$o(\Delta t)$である[91]。

［定理５－１］

いま仮定（１）～（３）を満足するｎ個の異なる入力事象$1, 2, \cdots n$からなる図５－２に示される順序依存形故障論理において、出力事象がある時刻ｔで生起している確率$Q^*(t)$、および出力事象の時刻ｔでの単位時間あたりの発生回数の期待値$w^*(t)$は

$$Q^*(t)=\sum_{x\in X_1}\Big[\int_0^t\int_{\tau_1}^t\int_{\tau_2}^t\cdots\int_{\tau_{n-1}}^t f_{x_1}(\tau_1)\cdot f_{x_2}(\tau_2)\cdots f_{x_n}(\tau_n)\,d\tau_n\,d\tau_{n-1}\cdots d\tau_1\Big] \tag{5-3}$$

$$w^*(t)=\sum_{x\in X_1}\Big[w_{x_n}(t)\int_0^t\int_{\tau_1}^t\int_{\tau_2}^t\cdots\int_{\tau_{n-2}}^t f_{x_1}(\tau_1)\cdot f_{x_2}(\tau_2)\cdots f_{x_{n-1}}(\tau_{n-1})\,d\tau_{n-1}\,d\tau_{n-2}\cdots d\tau_1\Big] \tag{5-4}$$

ここで

$$f_{x_i}(\tau_i)=w_{x_i}(\tau_i)\{1-G_{x_i}(t-\tau_i)\}$$

$$=\frac{\lambda_{x_i}}{\lambda_{x_i}+\mu_{x_i}}\left[\mu_{x_i}+\lambda_{x_i}\exp\{-(\lambda_{x_i}+\mu_{x_i})\tau_i\}\right]\exp\{-\mu_{x_i}(t-\tau_i)\} \tag{5-5}$$

により与えられる。

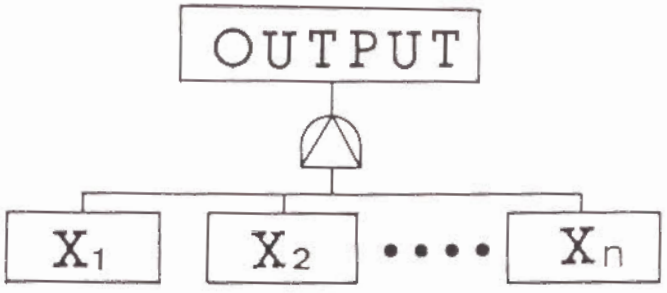


図５－２　基本的順序依存形故障論理

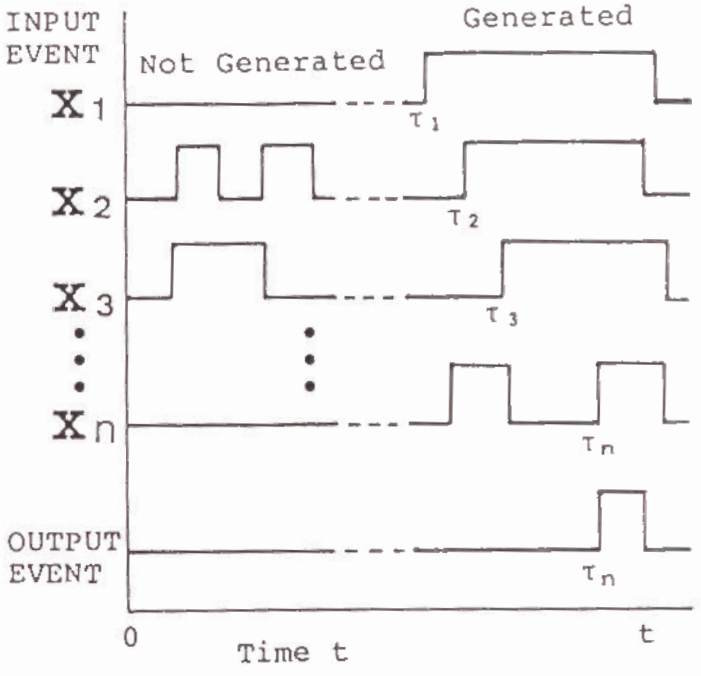


図５－３　順序依存形故障論理における入力事象と出力事象の関係

［証明］

時刻（0，t］をN等分して得られる微小区間$(t_j-\Delta t, t_j](j=1, 2, \cdots, N)$に順次1からNまでの番号を付け、微小区間を示すものとする。

事象 x_i の任意の微小区間biすなわち$(t_{bi}-\Delta t, t_{bi}]$での発生回数の期待値は

$$w_{x_i}(t_{bi})\Delta t+o(\Delta t)=Pr\{(t_{bi}-\Delta t, t_{bi}]で1回発生する\}+\sum_{m=2}^{\infty} m\cdot Pr\{(t_{bi}-\Delta t, t_{bi}]でm回発生する\} \quad (5-6)$$

と書けるが、仮定（1），（2）より上式右辺第2項は、$o(\Delta t)$となる。したがって、

$$Pr\{(t_{bi}-\Delta t, t_{bi}]で x_i が発生する\}=w_x(t_{bi})\Delta t+o(\Delta t) \quad (5-7)$$

ゆえに、入力事象 x_i が任意の微小区間biで発生し、それが少なくとも時刻tまで生起し続ける確率は

$$Pr\{(t_{bi}-\Delta t, t_{bi}]で x_i が発生する\}\cdot Pr\{少なくとも時刻tまで生起し続ける|(t_{bi}-\Delta t, t_{bi}]で発生する\}=w_{x_L}(t_{bi})\{1-G_x(t-t_{bi})\}\Delta t+o(\Delta t) \quad (5-8)$$

となる。

いま、事象E_iおよびA_iを次のように定める。

E_1：入力事象x_1が（0，t）で発生し、少なくとも時刻tまで生起し続ける。

E_i ：入力事象x_iが、x_{i-1}の時刻tで生起となる発生の後で発生し、少なくとも時刻tまで生起し続ける($i=2,3,\cdots$)。

A_i ：入力事象x_iが微小区間b_iで発生し、少なくとも時刻tまで生起し続ける。

すると、図5－3に例示するような$x \in X_1$なるある発生順序ベクトルxで入力事象が発生し、その結果出力事象が時刻tで生起している確率$Q_x^*(t)$は

$$Q_x^*(t) = P_r\{E_1 \cap E_2 \cap \cdots \cap E_n\} = \lim_{N\to\infty} \sum_{b_1=1}^{N-n+1} \sum_{b_2=b_1+1}^{N-n+2} \cdots \sum_{b_n=b_{n-1}+1}^{N} P_r\{A_1 \cap A_2 \cap \cdots \cap A_n\}$$

$$= \lim_{N\to\infty} \sum_{b_1=1}^{N-n+1} \sum_{b_2=b_1+1}^{N-n+2} \cdots \sum_{b_n=b_{n-1}+1}^{N} \{P_r(A_1)\cdot P_r(A_2|A_1)\cdot P_r(A_3|A_1\cap A_2)\cdots$$

$$\cdots P_r(A_n|A_1\cap A_2\cap\cdots\cap A_{n-1}\} \qquad (5-9)$$

仮定（1）より

$$Q_x^*(t) = \lim_{N\to\infty} \sum_{b_1=1}^{N-n+1} \sum_{b_2=b_1+1}^{N-n+2} \cdots \sum_{b_n=b_{n-1}+1}^{N} \{P_r(A_1)\cdot P_r(A_2)\cdots P_r(A_n)\} \qquad (5-10)$$

ここで

$$\tau_i = (b_{i-1}+m_i)\Delta t = \tau_{i-1} + m_i \Delta t,\ [m_i = 1,2,\cdots,\ (1-\frac{\tau_{i-1}}{t})N-(n-i),$$

$$\tau_0 \equiv 0,\ b_0 \equiv 0] \qquad (5-11)$$

とおくと、式（5－10）は、式（5－8）および　$t = t/N$より

$$Q_x^*(t)=\lim_{N\to\infty}\sum_{m_1=1}^{N-n+1}\sum_{m_2=1}^{(1-\tau_1/t)N-n+2}\cdots\sum_{m_n=1}^{(1-\tau_{n-1}/t)N}\Big[\,[w_{x_1}(m_1\Delta t)\{1-G_{x_1}(t-m_1\Delta t)\}\Delta t+o(\Delta t)]$$

$$\times[w_{x_2}(\tau_1+m_2\Delta t)\{1-G_{x_2}(t-\tau_1-m_2\Delta t)\}\Delta t+o(\Delta t)]$$

$$\cdots\cdot[w_{x_n}(\tau_{n-1}+m_n\Delta t)\{1-G_{x_n}(t-\tau_{n-1}-m_n\Delta t)\}\Delta t+o(\Delta t)]$$

$$=\int_0^t\int_{\tau_1}^t\int_{\tau_2}^t\cdots\int_{\tau_{n-1}}^t[w_{x_1}(\tau_1)\{1-G_{x_1}(t-\tau_1)\}w_{x_2}(\tau_2)\{1-G_{x_2}(t-\tau_2)\}\cdots$$

$$w_{x_n}(\tau_n)\{1-G_{x_n}(t-\tau_n)\}]d\tau_n d\tau_{n-1}\cdots\cdot d\tau_1 \qquad (5-12)$$

また、入力事象の発生順序ベクトルの集合は互いに排反事象の集合であるから

$$Q^*(t)=\sum_{x\in X}Q_x^*(t) \qquad (5-13)$$

よって式（５－３），（５－５）が成立する。

次に、入力事象が発生順序ベクトル $x\in X_1$ で生起することにより得られる出力事象の時刻 t での単位時間あたりの発生回数の期待値を $w_x^*(t)$ とする。

$w_x^*(t)$ に関して条件（１）～（３）より

$$\lim_{\Delta t\to 0}\frac{1}{\Delta t}\{w_x^*(t)\Delta t+o(\Delta t)\}=\lim_{\Delta t\to 0}\frac{1}{\Delta t}[Pr\{(0,t)\text{において、入力事象が}x_1,x_2,\cdots$$

$$,x_{n-1}\text{の順序で発生し、各々が少なくとも時刻 t まで生起しつづける}\}\,Pr\{[t,t+\Delta t)\text{で入力事象}x_n\text{が発生する}\}]$$

$$=\lim_{\Delta t\to 0}\frac{1}{\Delta t}\{w_{x_n}(t)\Delta t+o(\Delta t)\}\int_0^t\int_{\tau_1}^t\int_{\tau_2}^t\cdots\int_{\tau_{n-2}}^t f_x(\tau_1)\cdot f_x(\tau_2)\cdots$$

$$f_{x_{n-1}}(\tau_{n-1})d\tau_{n-1}d\tau_{n-2}\cdots\cdot d\tau_1 \qquad (5-14)$$

ゆえに

$$w_x^*(t)=w_{x_n}(t)\int_0^t\int_{\tau_1}^t\int_{\tau_2}^t\cdots\int_{\tau_{n-2}}^t f_{x_1}(\tau_1)\cdot f_{x_2}(\tau_2)\cdots$$

$$f_{x_{n-1}}(\tau_{n-1})d\tau_{n-1}d\tau_{n-2}\cdots d\tau_1 \qquad (5-15)$$

となり、式（５－１３）の場合と同様にして、式（５－４）が成立する［証明終わり］。

なお形式的に $X_1 = X$ としたときの $Q^*(t)$ および $w^*(t)$ に関して、それぞれ次式が成立する（証明省略）。

$$\prod_{i=1}^{n} Q_{x_i}(t)=\sum_{x\in X} Q_x^*(t)=\sum_{x\in X}\left[\int_0^t\int_{\tau_1}^t\int_{\tau_2}^t\cdots\int_{\tau_{n-1}}^t f_{x_1}(\tau_1)\cdot f_{x_2}(\tau_2)\cdots\right.$$

$$\left.\cdots f_{x_n}(\tau_n)d\tau_n d\tau_{n-1}\cdots d\tau_1\right] \qquad (5-16)$$

$$\sum_{j=1}^{n}\left[w_{x_j}(t)\left\{\prod_{\substack{i=1\\ i\neq j}}^{n} Q_{x_i}(t)\right\}\right]=\sum_{x\in X} w_x^*(t)=\sum_{x\in X}\left[w_{x_n}(t)\int_0^t\int_{\tau_1}^t\int_{\tau_2}^t\cdots\right.$$

$$\left.\cdots\int_{\tau_{n-2}}^t f_{x_1}(\tau_1)\cdot f_{x_2}(\tau_2)\cdots f_{x_{n-1}}(\tau_n)d\tau_n d\tau_{n-1}\cdots d\tau_1\right]$$

$$(5-17)$$

５．３．３　定常状態での一般解

式（５－３）および式（５－４）は、４～５入力事象ぐらいなら簡単に手計算で求まるが、ｎ入力事象とした一般解はまだ解かれていない。しかし定常解については以下に示すようにして与えられる。

$Q^*(t)$，$w^*(t)$ の定常解をそれぞれ Q_c^*，w_c^* とする。式（５－３），式（５－５）より

$$Q_c^* = \lim_{t\to\infty} Q^*(t) = \lim_{t\to\infty} \sum_{x\in X_1} \left[\left\{ \prod_{i=1}^{n} \frac{\lambda_{x_i}}{\lambda_{x_i}+\mu_{x_i}} \right\} \int_0^t \int_{\tau_1}^t \int_{\tau_2}^t \cdots \int_{\tau_{n-1}}^t \{\mu_{x_1}\exp(-\mu_{x_1}(t-\tau_1)) \right.$$

$$+\lambda_{x_1}\exp(-(\lambda_{x_1}+\mu_{x_1}t))\}\{\mu_{x_2}\exp(-\mu_{x_2}(t-\tau_2))+\lambda_{x_2}\exp(-(\lambda_{x_2}\tau_2+\mu_{x_2}t))\}$$

$$\left. \cdots\{\mu_{x_n}\exp(-\mu_{x_n}(t-\tau_n))+\lambda_{x_n}\exp(-(\lambda_{x_n}\tau_n+\mu_{x_n}t))\}\, d\tau_n d\tau_{n-1}\cdots d\tau_1 \right]$$

$$= \lim_{t\to\infty} \sum_{x\in X_1} \left[\left\{ \prod_{i=1}^{n} \frac{\lambda_{x_i}}{\lambda_{x_i}+\mu_{x_i}} \right\} \int_0^t \mu_{x_1}\exp(-\mu_{x_1}u_1) \int_0^{u_1} \mu_{x_2}\exp(-\mu_{x_2}u_2) \int_0^{u_2} \cdots \right.$$

$$\left. \int_0^{u_{n-1}} \mu_{x_n}\exp(-\mu_{x_n}u_n)\, du_n du_{n-1}\cdots du_1 \right] \qquad (5-18)$$

ところが

$$\int_0^{u_{i-1}} \mu_{x_i}\exp(-\mu_{x_i}u_i)\, du_i = L^{-1}\left\{ \frac{\mu_{x_i}}{s(s+\mu_{x_i})} \right\} \qquad (5-19)$$

であるから

$$Q_c^* = \lim_{t\to\infty} \sum_{x\in X_1} \left[\left\{ \prod_{i=1}^{n} \left(\frac{\lambda_{x_i}}{\lambda_{x_i}+\mu_{x_i}} \right) \right\} \quad L^{-1}\left\{ \frac{1}{s} \prod_{i=1}^{n} \left(\frac{\mu_{x_i}}{s+\sum_{j=1}^{i}\mu_{x_j}} \right) \right\} \right]$$

$$= \lim_{s\to 0} \sum_{x\in X_1} \left[\left\{ \prod_{i=1}^{n} \left(\frac{\lambda_{x_i}}{\lambda_{x_i}+\mu_{x_i}} \right) \right\} \quad L^{-1}\left\{ s\cdot \frac{1}{s} \prod_{i=1}^{n} \left(\frac{\mu_{x_i}}{s+\sum_{j=1}^{i}\mu_{x_j}} \right) \right\} \right]$$

$$= \sum_{x\in X_1} \left[\left\{ \prod_{i=1}^{n} \left(\frac{\lambda_{x_i}\mu_{x_i}}{\lambda_{x_i}+\mu_{x_i}} \right) \right\} \quad \left\{ \prod_{i=1}^{n} \left(\sum_{j=1}^{i}\mu_{x_j} \right) \right\}^{-1} \right] \qquad (5-20)$$

同様に

$$W_c^* = \sum_{x\in X_1} \left[\left\{ \prod_{i=1}^{n} \left(\frac{\lambda_{x_i}\mu_{x_i}}{\lambda_{x_i}+\mu_{x_i}} \right) \right\} \quad \left\{ \prod_{i=1}^{n-1} \left(\sum_{j=1}^{i}\mu_{x_j} \right) \right\}^{-1} \right] \qquad (5-21)$$

5．3．4　近似的非定常一般解

修理系では、$\lambda_{x_i}/\mu_{x_i} \ll 1$ $(i=1,2,\cdots\cdots,n)$ の場合が多く

$$\mu_{x_i}\exp\{-\mu_{x_i}(t-\tau_i)\}+\lambda_{x_i}\exp\{-(\lambda_{x_i}\tau_i+\mu_{x_i}t)\}$$

$$=\mu_{x_i}\exp\{-\mu_{x_i}(t-\tau_i)\}\left[1+\frac{\lambda_{x_i}}{\mu_{x_i}}\exp\{-(\lambda_{x_i}+\mu_{x_i})\tau_i\}\right]$$

$$\fallingdotseq\mu_{x_i}\exp\{-\mu_{x_i}(t-\tau_i)\} \qquad (i=1,2,\cdots,n) \qquad (5-22)$$

とした時の$Q^*(t)$，$w^*(t)$の近似的非定常一般解をそれぞれ$Q_a^*(t)$，$w_a^*(t)$とすると、式（5－3），式（5－5）より

$$Q_a^*(t)=\sum_{x\in X_1}\left[\left(\prod_{i=1}^{n}\frac{\lambda_{x_i}}{\mu_{x_i}}\right)\int_0^t\mu_{x_1}\exp(-\mu_{x_1}u_1)\int_0^{u_1}\mu_{x_2}\exp(-\mu_{x_2}u_2)\int_0^{u_2}\cdots\right.$$

$$\left.\int_0^{u_{n-1}}\mu_{x_n}\exp(-\mu_{x_n}u_n)\,du_1du_2\cdots du_n\right] \qquad (5-23)$$

ところが式（5－19）より

$$Q_a^*(t)=\sum_{x\in X_1}\left[\left(\prod_{i=1}^{n}\frac{\lambda_{x_i}}{\mu_{x_i}}\right)L^{-1}\left\{\frac{1}{s}\prod_{i=1}^{n}\left(\frac{\mu_{x_i}}{s-(-a_i)}\right)\right\}\right]$$

$$=\sum_{x\in X_1}\left[\left(\prod_{i=1}^{n}\lambda_{x_i}\right)\sum_{k=0}^{n}\left\{\frac{\exp(-a_kt)}{\prod_{\substack{j=0\\j\neq k}}^{n}(a_j-a_k)}\right\}\right] \qquad (5-24)$$

ただし、ここで

$$a_m\equiv\sum_{i=1}^{m}\mu_{x_i}\quad(m=1,2,\cdots,n),\quad a_0\equiv0,\quad a_j\neq a_k$$

とする。

$w_a^*(t)$ も同様に

$$w_a^*(t)=\sum_{x\in X_1}\left[\left(\prod_{i=1}^{n}\lambda_{x_i}\right)\sum_{k=0}^{n-1}\left\{\frac{\exp(-a_k t)}{\prod_{\substack{j=0\\ j\neq k}}^{n-1}(a_j-a_k)}\right\}\right] \qquad (5-25)$$

5．3．5　r/n 順序依存形故障論理のアルゴリズム

前節までにおいては、優先ＡＮＤゲートへの全ての入力事象の発生順序が出力事象の生起に影響する場合の定量化アルゴリズムを検討してきた。実際の系では、図５－４に示すようにｎ個の入力事象のうちｒ個の入力事象x_i(i=1, 2, ･･･, r) の発生順序のみが出力事象の生起に関係し、他の（ｎ－ｒ）個の入力事象y_j(j=1, 2, ･･･, n-r) の発生順序は無関係となる場合がある。このような場合でも、全ての入力事象の発生順序について検討する前節までのアルゴリズムを適用して、出力事象の期待発生回数などの特性値を計算できるが、以下のようなアルゴリズムを用いることにより、計算が効率化される[92]。

［定義５－１］ｎ個の入力事象ｉ(i=1, 2, ･･･, n) からなる、あるカットにおいて、出力事象を生起させる入力事象の発生順序ベクトル$x\in X_1$がξ個存在するとする。各々の発生順序ベクトルｘ中のある入力事象ｊを除去して他の入力事象の相対的順序はそのままにして得られる（ｎ－１）次元のベクトルx_jの集合を$X_{1,j}$とする。入力事象ｊを除去することにより、$X_{1,j}$の中にｎ個の同一のベクトルがｐ(p=1, 2, ･･･) 組存在するとき、入力事象ｊをそれらｐｎ個のx_jの元のベクトルｘに関する可除去入力という。可除去入力でない入力事象を不可除去入力という。

［定義５－２］ある発生順序ベクトルｘがｒ個の不可除去入力から構成されているとする。それら不可除去入力の相対的順序をそのままにし、（ｎ－ｒ）個の可除去入力を全てｘより取り除いてできるｒ次元の発生順序ベクトルを相等

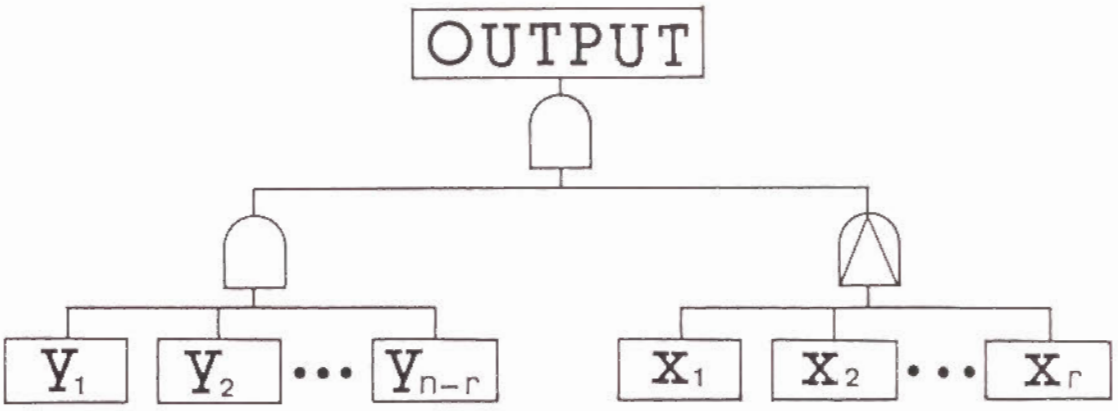


図５－４　ｒ／ｎ順序依存形故障論理の図式表現

しいものはそれぞれ同一のベクトルとして、η（$\eta \leq \xi$）個の相違なる発生順序ベクトル

$$x_{min} = (x_1, x_2, \cdots, x_r) \tag{5-26}$$

で表し、x_{min} の全集合をX_{1r}とする。

さらに、可除去入力をそれぞれ$y_1, y_2 \cdots y_{n-r}$ で表す。

［定義５－３］図５－４に示すような（ｎ－ｒ）個の可除去入力によるＡＮＤ構造と、ｒ個の不可除去入力によるPriority-AND構造とのＡＮＤ結合によって表される最小カットの出力構造を、r/n 順序依存形故障論理と言う。

［定理５－２］

いま、5.3.2 節の仮定（１）～（３）を満足するｎ個の相異なる入力事象1, 2･･･n からなるカットが、η 個のr/n 順序依存形故障論理によって構成されるとき、出力事象がある時刻ｔで生起している確率$Q^*(t)$、および出力事象の時刻ｔでの単位時間あたりの発生回数の期待値$w^*(t)$は

$$Q^*(t)=\sum_{x_{min}\in X_{1r}}\Big[\Big\{\int_0^t\int_{\tau_1}^t\int_{\tau_2}^t\cdots\int_{\tau_{r-1}}^t f_{x_1}(\tau_1)\cdot f_{x_2}(\tau_2)\cdots f_{x_r}(\tau_r)\,d\tau_r\,d\tau_{r-1}\cdots d\tau_1\Big\}\Big\{\prod_{j=1}^{n-r}Q_{y_j}\Big\}\Big] \tag{5-27}$$

$$w^*(t)=\sum_{x_{min}\in X_{1r}}\Big[w_{x_r}\Big\{\int_0^t\int_{\tau_1}^t\int_{\tau_2}^t\cdots\int_{\tau_{r-2}}^t f_{x_1}(\tau_1)\cdot f_{x_2}(\tau_2)\cdots f_{x_{r-1}}(\tau_{r-1})\,d\tau_{r-1}\,d\tau_{r-2}\cdots d\tau_1\Big\}\Big\{\prod_{j=1}^{n-r}Q_{y_j}\Big\}\Big] \tag{5-28}$$

ここで $f_{x_k}(\tau_k)$ $(k=1,2,\cdots,r)$ は式（５－５）によって定義され

$$Q_{y_j}=\int_0^t w_{y_j}(\tau)\{1-G_{y_j}(t-\tau)\}\,d\tau$$

$$=\frac{\lambda_{y_j}}{\lambda_{y_j}+\mu_{y_j}}\left[1-\exp\{-(\lambda_{y_j}+\mu_{y_j})t\}\right] \tag{5-29}$$

さらに、$w_{y_j}(\tau)$，$G_{y_j}(t-\tau)$，λ_{y_j}，μ_{y_j} はそれぞれ可除去入力 y_j $(j=1,2,\cdots,n-r)$ の、時刻 τ での単位時間あたりの発生回数の期待値、時刻 τ での発生による生起が時刻 t までに修復している確率、時刻 t での非生起条件下での単位時間あたりの発生確率、同じく生起条件下での単位時間あたりの修復確率とする。

［証明］　省略

r/n順序依存形故障論理における $Q^*(t)$，$w^*(t)$ の定常状態での一般解をそれぞれ Q_0^*，w_0^* とすると

$$Q_0^*=\sum_{x_{min}\in X_{1r}}\Big[\Big\{\prod_{i=1}^{r}\Big(\frac{\lambda_{x_i}\mu_{x_i}}{\lambda_{x_i}+\mu_{x_i}}\Big)\Big\}\Big\{\prod_{k=1}^{r}\Big(\sum_{\ell=1}^{k}\mu_{x_\ell}\Big)\Big\}^{-1}\times\Big\{\prod_{j=1}^{n-r}\Big(\frac{\lambda_{y_j}}{\lambda_{y_j}+\mu_{y_j}}\Big)\Big\}\Big] \tag{5-30}$$

$$w_c^* = \sum_{x_{min} \in X_{1r}} \left[\left\{ \prod_{i=1}^{r} \left(\frac{\lambda_{x_i} \mu_{x_i}}{\lambda_{x_i} + \mu_{x_i}} \right) \right\} \left\{ \prod_{k=1}^{r-1} \left(\sum_{\ell=1}^{k} \mu_{x_\ell} \right) \right\}^{-1} \right.$$

$$\left. \times \left\{ \prod_{j=1}^{n-r} \left(\frac{\lambda_{y_j}}{\lambda_{y_j} + \mu_{y_j}} \right) \right\} \right] \qquad (5-31)$$

また入力事象kについて、$\lambda_k / \mu_k \ll 1 \quad (k=1, 2, \cdots, n)$のとき、$Q^*(t)$, $w^*(t)$の近似的非定常一般解を$Q_a^*(t)$, $w_a^*(t)$とすると

$$Q_a^*(t) = \sum_{x_{min} \in X_{1r}} \left[\left[\left(\prod_{i=1}^{r} \lambda_{x_i} \right) \sum_{k=0}^{r} \left\{ \frac{\exp(-a_k t)}{\prod_{\substack{\ell=0 \\ \ell \neq k}}^{r} (a_\ell - a_k)} \right\} \right] \left[\prod_{j=1}^{n-r} \left(\frac{\lambda_{y_j}}{\mu_{y_j}} \right) \{1 \right. \right.$$

$$\left. \left. - \exp(-\mu_{y_j} t) \} \right] \right] \qquad (5-32)$$

$$w_a^*(t) = \sum_{x_{min} \in X_{1r}} \left[\left[\left(\prod_{i=1}^{r} \lambda_{x_i} \right) \sum_{k=0}^{r-1} \left\{ \frac{\exp(-a_k t)}{\prod_{\substack{\ell=0 \\ \ell \neq k}}^{r-1} (a_\ell - a_k)} \right\} \right] \left[\prod_{j=1}^{n-r} \left(\frac{\lambda_{y_j}}{\mu_{y_j}} \right) \{1 \right. \right.$$

$$\left. \left. - \exp(-\mu_{y_j} t) \} \right] \right] \qquad (5-33)$$

ただし

$$a_m \equiv \sum_{k=1}^{m} \mu_{x_k} \quad (m=1, 2, \cdots, r), \quad a_0 \equiv 0, \quad a_\ell \neq a_k$$

とする。

5．3．6　定常解と厳密解から求めた発生回数の期待値の比較

安全性の評価で実際に意味をもつのは、望ましくない事象である出力事象がある時間長あたりにどの程度発生するかの指標、すなわち出力事象の発生回数の期待値である。時刻0で全ての入力事象が非生起の条件下で、時刻tまでの出力事象の発生回数の期待値を求めるための厳密式を$W^*(0,t)$，また定常解を用いて得られる近似式を$W_c^*(0,t)$とする。発生回数の期待値を定常解を用いた近似式で求めたとき、どの程度の誤差が生ずるかを、3入力事象 1,2,3、$X_1=[1,2,3]$，$\lambda_1=\lambda_2=\lambda_3=10^{-4}$［時間$^{-1}$］，$\mu_1=\mu_2=\mu_3=60$［時間$^{-1}$］の場合を例にとって検討する。

式（5－4）および$\lambda_1\neq\mu_2$、$\lambda_2\neq\mu_1$、$W^*(0,0)=0$より、$W^*(0,t)$は

$$W^*(0,t)=\int_0^t w^*(\tau)d(\tau)=\left\{\prod\left(\frac{\lambda_i}{\lambda_i+\mu_i}\right)\right\}\left[\left\{\left(\frac{\mu_2}{\mu_1+\mu_2}\right)t+\frac{\mu_2\exp(-(\lambda_1+\mu_1)t)}{(\mu_2-\lambda_1)(\lambda_1+\mu_1)}+\frac{\lambda_2\exp(-(\lambda_2+\mu_2)t)}{(\lambda_2-\mu_1)(\lambda_2+\mu_2)}\right.\right.$$

$$-\left(\frac{\lambda_1}{\lambda_1+\lambda_2}+\frac{\mu_1}{\mu_1+\mu_2}+\frac{\mu_1}{\lambda_2-\mu_1}+\frac{\lambda_1}{\mu_2-\lambda_1}\right)$$

$$\left.\left.\times\frac{\exp(-(\mu_1+\mu_2)t)}{\mu_1+\mu_2}-\frac{\lambda_2\exp(-(\lambda_1+\mu_1+\lambda_2+\mu_2)t)}{(\lambda_1+\lambda_2)(\lambda_1+\mu_1+\lambda_2+\mu_2)}\right\}\mu_3\right.$$

$$+\left\{-\frac{\mu_2\exp(-(\lambda_3+\mu_3)t)}{(\mu_1+\mu_2)(\lambda_3+\mu_3)}+\frac{\mu_2\exp(-(\lambda_1+\mu_1+\lambda_3+\mu_3)t)}{(\mu_2-\lambda_1)(\lambda_1+\mu_1+\lambda_3+\mu_3)}\right.$$

$$+\frac{\lambda_2\exp(-(\lambda_2+\mu_2+\lambda_3+\mu_3)t)}{(\lambda_2-\mu_1)(\lambda_2+\mu_2+\lambda_3+\mu_3)}-\left(\frac{\lambda_1}{\lambda_1+\lambda_2}+\frac{\mu_1}{\mu_1+\mu_2}+\frac{\mu_1}{\lambda_2-\mu_1}\right.$$

$$\left.\left.+\frac{\lambda_1}{\mu_2-\lambda_1}\right)\frac{\exp(-(\mu_1+\mu_2+\lambda_3+\mu_3)t)}{\mu_1+\mu_2+\lambda_3+\mu_3}\right.$$

$$- \frac{\lambda_2 \exp(-(\lambda_1+\mu_1+\lambda_2+\mu_2+\lambda_3+\mu_3)t)}{(\lambda_1+\lambda_2)(\lambda_1+\mu_1+\lambda_2+\mu_2+\lambda_3+\mu_3)} \} \lambda_3$$

$$- \{ \frac{\mu_2}{(\mu_2-\lambda_1)(\lambda_1+\mu_1)} + \frac{\lambda_2}{(\lambda_2-\mu_1)(\lambda_2+\mu_2)}$$

$$- \left(\frac{\lambda_1}{\lambda_1+\lambda_2} + \frac{\mu_1}{\mu_1+\mu_2} + \frac{\mu_1}{\lambda_2-\mu_1} + \frac{\lambda_1}{\mu_2-\lambda_1} \right) \frac{1}{\mu_1+\mu_2}$$

$$- \frac{\lambda_2}{(\lambda_1+\lambda_2)(\lambda_1+\mu_1+\lambda_2+\mu_2)} \} \mu_3 - \{ - \frac{\mu_2}{(\mu_1+\mu_2)(\lambda_3+\mu_3)}$$

$$+ \frac{\mu_2}{(\mu_2-\lambda_1)(\lambda_1+\mu_1+\lambda_3+\mu_3)} + \frac{\lambda_2}{(\lambda_2-\mu_1)(\lambda_2+\mu_2+\lambda_3+\mu_3)}$$

$$- \left(\frac{\lambda_1}{\lambda_1+\lambda_2} + \frac{\mu_1}{\mu_1+\mu_2} + \frac{\mu_1}{\lambda_2-\mu_1} + \frac{\lambda_1}{\mu_2-\lambda_1} \right) \frac{1}{\mu_1+\mu_2+\lambda_3+\mu_3}$$

$$- \frac{\lambda_2}{(\lambda_1+\lambda_2)(\lambda_1+\mu_1+\lambda_2+\mu_2+\lambda_3+\mu_3)} \} \lambda_3] \qquad (5-34)$$

$W_c^*(0,t)$ は、式（５－２１）より（ｎ＝３の場合）

$$W_c^*(0,t) = \int_0^t w_c^* dt = \{ \prod_{i=1}^{3} \left(\frac{\lambda_i}{\lambda_i+\mu_i} \right) \} \left(\frac{\mu_2\mu_3}{\mu_1+\mu_2} \right) t \qquad (5-35)$$

ここで誤差率 $\gamma^*(t)$ を

$$\gamma^*(t) \quad [W^*_c(0,t)-W^*(0,t)]/W^*(0,t) \qquad (5-36)$$

とすると、t=1,10,100［時間］でそれぞれ、

$\gamma^{*}(t) = 2.56\times10^{-2},\ 2.51\times10^{-3},\ 2.50\times10^{-4}$

となる。

このように高信頼度系でＭＴＴＲ(Mean Time to Repair)が小さい系では、ある程度の時間長での出力事象の発生回数の評価として、算定値が多少大きくなるが、系の安全性評価上は厳しく見積ることとなるので、実用上、定常解より得られる近似式を用いることで十分であると考えられる。

５．３．７　考　察

5-2 節で論じたカットの例では、「人間の侵入」（Nb05）がロボットの腕の動作を停止させ（インターロッキングが正常のとき）、その後の「制御系への動作命令の発生」（Ee16）の頻度などに影響を与えることが考えられる。しかし、このような場合でも、系が高信頼度系であり、例えば事象Nb05したがって出力事象の発生回数が十分小さいとき、それらの事象の相互の干渉による影響は軽微な範囲に止まり、ＫＩＴＴ(Kinetic Tree Theory) などで行われているように入力事象間での相互の統計的独立性を仮定してもよいものと考えられる[93]。しかし、それらの影響を無視できないときは本アルゴリズムをそのままでは適用できない。

本アルゴリズムでは、入力事象x_iが発生するときのx_i以降の発生順序をもつ事象x_j(j=i+1, i+2･･･, n)の生起・非生起については何も規定していない。一般的に考えれば、x_iが発生するときに、いくつかのx_jが非生起の状態にあることが必要条件として抑制ゲート中に含まれる場合もあり得る。そのようなx_jはその状態以降の発生確率などがその条件による条件付き確率によって与えられるため、本アルゴリズムで与えた$f_{x_j}(\tau_j)$とは異なってくる。しかし、x_jの生起している確率が十分小さいときはx_j がx_i の発生時に生起しており、かつ非生起状態となり、再び時刻ｔまでに生起の状態となる確率は非常に小さくなる。

したがって本アルゴリズムによって与えられるものは、そのような抑制ゲートの条件を加味したものとほとんど数量的には一致すると考えてよいであろう。

本アルゴリズムの具体的なカットへの適用にあたっては、以上の点に注意しなければならない。

５．４　結　　言

人間－ロボット系の安全性評価では、順序依存形故障論理（およびr/n 順序依存形故障論理）が重要であることをＦＴより具体的に示した。順序依存形故障論理の入力事象に本章で与えた仮定を置くことが可能ならば、提案されたアルゴリズムにより、出力事象が時刻ｔで生起している確率および単位時間あたりの発生回数の期待値を求めることができる。従来は修理系での順序依存形故障論理のアルゴリズムとしては、Markovのモデルの適用が原理的に考えられていたが、入力事象の数に制約を受け、一般解は得られていない。本章では、その定常状態での一般解および非定常状態での近似的一般解を与えた。本アルゴリズムは、出力事象の発生回数の期待値を求めるうえで、Markovモデルに比較し、はるかに簡便であると言える。本アルゴリズムは、単一のカットについてのものであるが、これを一般的なＦＴＡの技法と直ちには同様に扱えない。これは今後の研究課題となろう。

第６章　無人加工セルの安全性評価

６．１　緒　　言

前章までにおいて、人間－ロボット系の安全性評価に必要な潜在危険の同定と抑制論、災害発生機構の解析のための包括的論理モデルおよびその定量化のためのアルゴリズムなど、基本的または一般化された方法論について論じた。個々の系の安全性評価は、それらの方法論を系の具体的な諸条件に従って特殊化することによって行われる。

本章では、産業用ロボットおよびNC（数値制御）マシンなどから構成される具体的な加工セルを取り上げ、これまでに述べた方法論を用いて安全性評価を実施する。これにより、安全性評価の遂行のために、それら基本的方法論がいかに有機的に関連づけられるか、また系の具体的な諸条件に従って一般化された方法論がどのように特殊化されるかを例示するとともに、それら方法論の有効性を検証する。

６．２　系の設定

次のような、産業用ロボットおよびNCマシンを用いた加工セルを設定する。ただし、本章では、以下において、系の相を「自動運転モード（ロボットの運転状態特性）」からなる相に限定して検討する（第４章、図４－７参照）。

６．２．１　ロボットの自動運転モード

ある機械工場における加工セルでは、NCマシン、ロボット、加工物送給機そして加工物搬出コンベアなどが図６－１のように配置されている。

ロボットの自動運転による作業は、その開始信号とともに、図６－１の位置

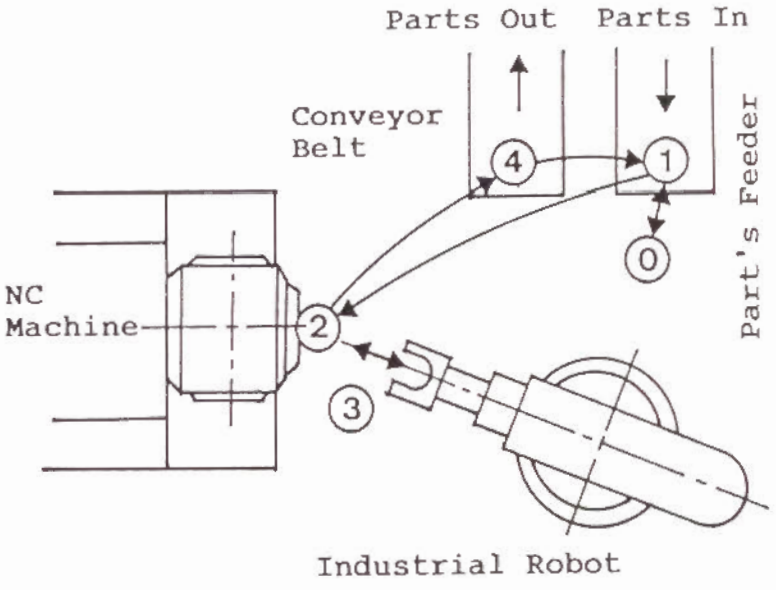

Parts Out
Parts In
Conveyor
Belt
4
1
0
Part's Feeder
NC
Machine
2
3
Industrial Robot

図６－１　無人加工セル

⓪で待機していたマニプレータの把持部が作動し、加工物送給機上の位置①より室温の金属からなる加工物をつかみあげ、マニプレータが、これを把持したままNCマシンへのセット位置②まで旋回して、加工物をNCマシンへセットすることにより開始される。

マニプレータは、加工物が加工される間、セット位置②よりやや離れた位置③で把持部を待機させ、NCマシンより加工完了の信号を受けとるとともに、再びセット位置②で加工物を取り出す。さらに、これを把持したまま旋回して、加工物搬出コンベア上の位置④まで搬送する。

作業が1ブロック・シーケンスで行われる場合には、ロボットは、ここでマニプレータの把持部を元の位置⓪へ戻し、再び作業開始操作が行われるまで、その動力源を遮断した状態で停止する。

作業が連続自動運転で行われる場合には、ロボットは、さらに位置④より位置①まで把持部を移動させ、すでに加工物送給機によって供給されている次の加工物をつかみあげ、セット位置②でNCマシンにセットし、以下、位置③で待機、位置②で取り出し、位置④まで搬送と、同様の作業を作業終了の信号が与えられるまでくり返し行う。

作業者が、通常の方法でロボットを停止させるためには、ロボットの運転モードを連続自動運転から1ブロック・シーケンスに切換える操作を行い、これによって、ロボットはNCマシンで加工完了となった加工物を位置④まで搬送した後、把持部を位置⓪に戻し、動力源を切断した状態で完全に停止する。

6．2．2　作業者が危険域へ必要上接近して存在するモード

当該加工工程は、連続自動運転時において、通常無人で作業が行われる。しかし、時として、ロボットの落とした加工物の処理など異常処理作業を行うために、作業者がマニプレータの作動域である危険域内へ立ち入る必要性が生ずることがある。ただし、加工物の落下などの異常が生じても、無人加工セルの連続自動運転モードは自動的には解消されず、作業は続行される。

6．2．3　作業者が危険域へ不必要に侵入して存在するモード

作業者が不必要に侵入して存在するモードがある。これは、第4章、図4-6における事象Ne01、Ne02、Ne03、Ne04などの異常モードにより生ずる。

6．3　潜在危険の同定

ロボットの人間に対する潜在危険には、種々のものが第2章において同定された。このうち、前節で設定された系の条件より、第1に考慮すべき潜在危険として、マニプレータの自律的運動の結果生ずる運動エネルギーが作業者へ直接原因作用として働くものが挙げられる（実際に、この直接原因作用による災害が発生している[94]）。この直接原因作用をもたらす潜在危険は、A－Cモデルにより、図6－2のように同定される。

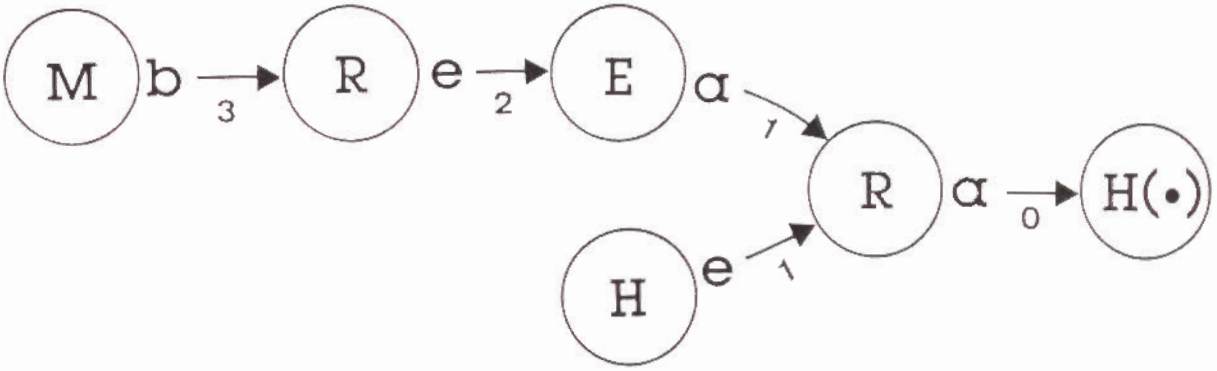
ここで、H，R，M，Eは、それぞれ系の要素、作業者、ロボット、NCマシン、そしてロボットの動力源を示す。

NCマシンMからロボットへ加工完了の信号が送られ［$Mb \xrightarrow{3}$］、ロボットが作動のための動力源を受けとる状態となり［$Re \xrightarrow{2}$］、動力源Eよりロボットへ作動のための動力が供給される［$Ea \xrightarrow{1}$］。このとき、作業者Hがマニプレータに打たれる危険域に存在するため［$He \xrightarrow{1}$］、ロボットから作業者へ直接原因作用がもたらされる［$Ra \xrightarrow{0}$］。

この直接原因作用により、作業者がマニプレータによって打たれる災害が発生する。本章では、以下この潜在危険について検討する。

6．4　潜在危険制御系の構成

第3章で論じた潜在危険制御系の構成法則に基づき、前節で同定された潜在危険に対して、侵入防止機構、手動停止機構および自動インターロッキング機構などからなる潜在危険制御系を構成する。



System elements

H : Human　R : Robot　E : Robot energy source

M : NC machine

Action links

a ⟶: Energy-transmission type action-link

b ⟶: Information-propagation type action-link

e ⟶: Existence-form type action-link

図６－２　潜在危険の同定

6．4．1　不必要な侵入の防止

前節で同定された潜在危険において、作用鎖［$He \xrightarrow{1}$］は作用鎖［$Ra \xrightarrow{0}$］の必要条件となっている。そこで、［$He \xrightarrow{1}$］を解離すれば直接原因作用の発現を防ぐことができる。

これを実現する潜在危険制御系が、次の制御連鎖などにより構成できる［第3章、構成則3－1］：

$$Wu_1' \xrightarrow{2} He \overset{P_1}{\not\xrightarrow{1}} R \qquad (6\text{-}1)$$

ここでWは、図6－3に示すような加工セルの周囲に張り巡らした金網として具体化される。金網は、作業者などの不必要な侵入を防止するとともに、ロボットが加工物の把持に失敗することにより、加工物を外部へ飛来・衝突させる潜在危険をも抑制する。加工セルの中へは、必要に応じて、図中に示すような戸扉を開けて入ることができるが、通常これは施錠され、専任の作業者のみに鍵の管理が委ねられる。

6．4．2　動力源の遮断による潜在危険制御系

誘因作用鎖［$Ea \xrightarrow{1}$］は、原理的に解離原理P_1で解離される［構成則3－1］。この解離を実現して、同定された潜在危険による災害を防止する潜在危険制御系は以下のように構成される。

a．手動停止機構による潜在危険制御系

作業者がロボットの運転モードを1ブロック・シーケンスへ切換えると、1ブロック・シーケンス終了後、誘因作用鎖［$Ea \xrightarrow{1}$］が解離される。さらに、作業者が1ブロック・シーケンス終了前には危険域内に立ち入ることを自ら抑制することによって、1ブロック・シーケンスが終了する以前に生ずる誘因作用鎖［$He \xrightarrow{1}$］が解離されなければならない。すなわち、この場合、

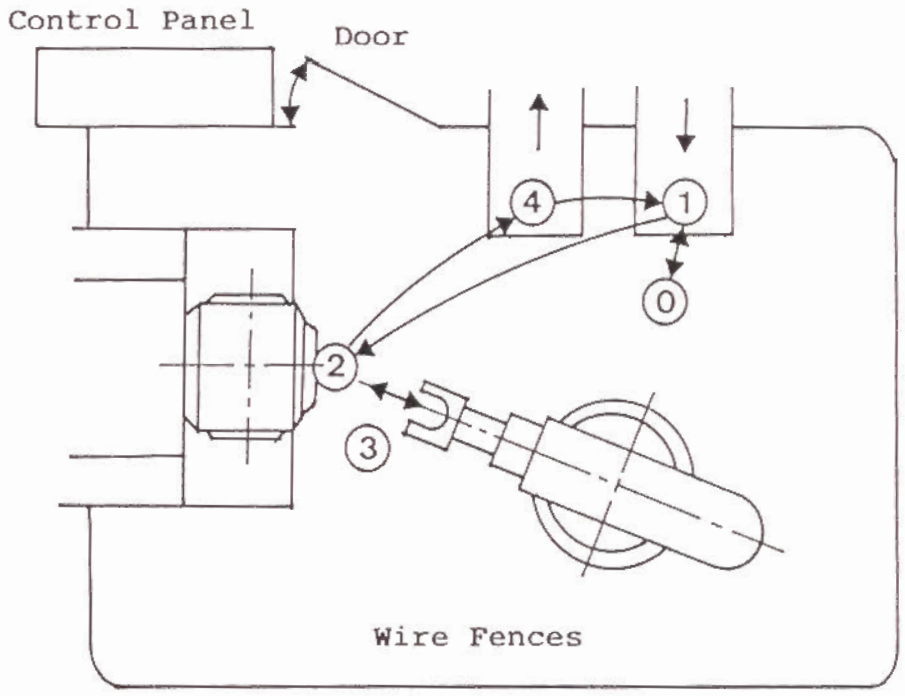


図６－３　手動停止機構の概念化

潜在危険を完全に抑制するには、少なくとも２本の誘因作用鎖が解離されることが必要である〔第３章、性質３－６〕。これらの潜在危険制御系は、次の制御連鎖などからを構成される：

$$Hb'' \xrightarrow{-3} Cu_i' \xrightarrow{-2} Ea \overset{P_1}{\not\xrightarrow{1}} R \qquad (6\text{-}2)$$

$$Rb'' \xrightarrow{-3} He' \xrightarrow{-2} He \overset{P_1}{\not\xrightarrow{1}} R \qquad (6\text{-}3)$$

作業者Ｈは、通常のロボット停止を行うとき、セル内への戸扉横に設置されている操作盤で，ロボットの運転モードを連続自動運転から１ブロック・シーケンスに切り替える［$Hb'' \xrightarrow{-3}$］。すると、操作盤制御部Ｃが、１ブロック・シーケンス終了後、動力源を遮断する［$Cu_i' \xrightarrow{-2}$］。また、作業者は１ブロック・シーケンス終了前には［$Rb'' \xrightarrow{-3}$］、危険域に立ち入らないようにする必要がある［$He' \xrightarrow{-2}$］。

ｂ．自動インターロッキング機構による潜在危険制御系

誘因作用鎖［$Ea \xrightarrow{1}$］を操作盤上の手動操作によらず解離するためには、次の制御連鎖の成立が必要である［構成則３－１］：

$$Hu_i'' \xrightarrow{-5} Su_j'' \xrightarrow{-4} Pu_k'' \xrightarrow{-3} Au_l' \xrightarrow{-2} Ea \overset{P_1}{\not\xrightarrow{1}} R \qquad (6\text{-}4)$$

作業者Ｈの危険域への侵入［$Hu_i'' \xrightarrow{-5}$］を、センサＳが検出して処理部Ｐへ抑制作用を伝播する［$Su_j'' \xrightarrow{-4}$］。すると、処理部から出力部Ａへ抑制作用［$Pu_k'' \xrightarrow{-3}$］が伝播され、これにより、出力部が、直ちに、動力源

を遮断する解離作用を発生する［$Au_1' \xrightarrow{-2}$］。

この潜在危険制御系では、旋回しているマニプレータを強制的に停止させる緊急制動機構が考慮されていない。従って、作業者がマニプレータの惰性運動により打たれる危険を避けるためには、マニプレータの惰性運動中の誘因作用鎖［$He \xrightarrow{-1}$］が解離されなければならない。これは、次の制御連鎖により実現される［構成則３－１］：

$$Rb'' \xrightarrow{-3} He' \xrightarrow{-2} He \overset{P_1}{\not\longrightarrow} R \qquad (6\text{-}5)$$

すなわち、この場合でも、潜在危険を完全に抑制するためには、少なくとも２本の誘因作用鎖が解離されなければならない〔性質３－６〕。　動力源遮断のための潜在危険制御系は、自動インターロッキング機構として図６－４のように概念化される。

制御連鎖(6-4) では、動力源の遮断により生ずる潜在危険が無視できるものとすれば、各作用鎖を動力源の遮断方向のみの単方向制御作用鎖とすることができる［構成則３－８］。従って、この場合の情報処理系は可フェイル・セーフ形または可フォールト・トレラント形のいずれも原理的に構成可能である［構成則３－７］。

本章では、可フェイル・セーフ形情報処理系を採用する。すると、制御連鎖(6-4) は次のように書き換えられる。

$$He'' \xrightarrow{-5} Sf'' \xrightarrow{-4} Pf'' \xrightarrow{-3} Af' \xrightarrow{-2} Ea \overset{P_1}{\not\longrightarrow} R \qquad (6\text{-}6)$$

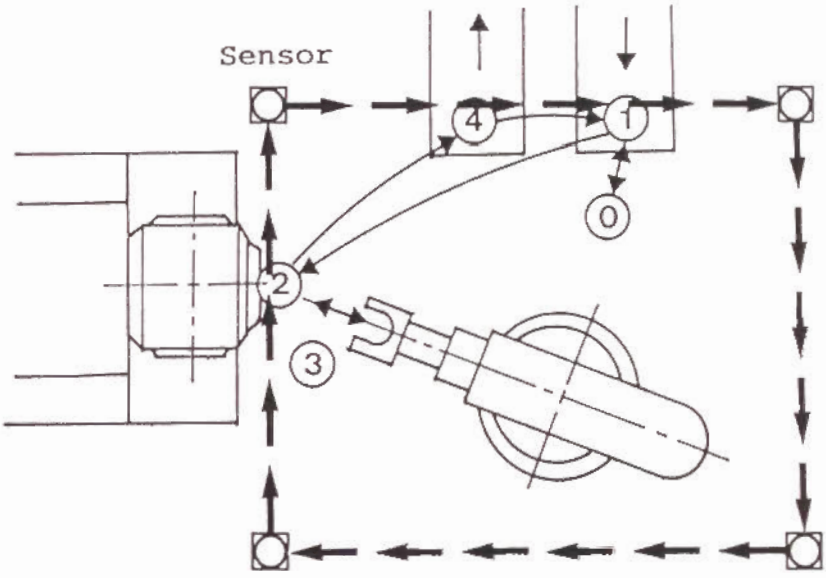


図６－４　自動インターロッキング機構センサ系の概念化

６．５　定性的安全性解析

本節以降では、系の相を「ロボットの自動運転モード」と「作業者が必要上接近して存在するモード」からなる相に限定し（第４章、図４－７参照）、同定された潜在危険による災害の発生論理を解析する。

６．５．１　制御連鎖の反転

潜在危険制御系を構成する各要素に、ヒューマン・エラーや故障が発生すると以下のように制御連鎖が反転して解離が実現されない。

ａ．手動停止機構

（１）作業者がセルに入る際に、操作盤でのロボット停止操作を怠ると、制御連鎖(6-2）が反転して解離が実現されない。その他、操作盤や動力源などのハードウェアの故障による反転も想定されるが、それらはヒューマン・エラーに比して無視できる程度であるものとし、本章では省略する。

（２）作業者がロボット停止操作を行うものの、１ブロック・シーケンス終了を待たずにセル内に入ると、制御連鎖(6-3）が反転して解離が実現されない。

その他、ロボットの完全停止後に入るものの、第三者がロボットの起動操作を行ってしまう異常モードも想定されるが、本章では省略する。

ｂ．自動インターロッキング機構

（１）自動インターロッキング機構情報処理系の故障には、一般に、誤って動力源を遮断する故障と、動力源を遮断できなくなる故障モードが存在する。ここで問題にしている潜在危険では、後者の故障モードがいわゆる危険側の故障となる。危険側の故障が発生すると、制御連鎖(6-6）が反転して解離が実現されない。この故障には、制御連鎖(6-6）の［Ｈｅ”$\xrightarrow[5]{}$］を反転させるものも含むものとする。

（２）動力源を構成するハードウェアに、誤って動力を供給してしまう故障が

発生すると、同様に解離が実現されない。

その他、マニプレータの惰性運動中に危険域に入るヒューマン・エラーが発生すると、制御連鎖(6-5)が反転して解離が実現されなくなるが、マニプレータが動作しているときの侵入の発生は、マニプレータが停止している場合の侵入の発生に比べて相対的に軽微であり無視できるものとする。

6．5．2　災害発生論理のＦＴ

個々の系の災害発生論理は、第４章で作成した論理モデルを具体的な系の諸条件に従って特殊化することによって得られる。ここでは、マニプレータの強度、速度、出力などは、災害を生じさせるに十分なほど大きいものとして、災害発生論理のＦＴを求める。以下で用いるＦＴの事象識別記号は、第４章のものと一致する。

ａ．手動停止機構のみを備えた系

Case（a-1）：停止操作を怠ることによる災害発生論理

「マニプレータ作動」（Eb10）事象は、加工物の加工完了による「停止条件の解消」（Ef24）によって生ずる「動作信号」（Ed09）事象、インターロッキングを行う自動停止機構の「不設置」（Ee21）常起事象、および「停止のための操作を怠る」（Ed11,1）ことによる「動力源の存在」（Ed11）事象がすべて生起することにより生ずる。

頂上事象「マニプレータによって打たれる」（Ea04）は、「防護の不設置」（Oa02）常起事象、「異常処理作業」（Nc09）による「危険域に存在」（Eb12）事象、および「マニプレータの作動」（Eb10）事象がすべて生起することにより生ずる。

Case（a-2）：完全停止の確認を怠ることによる災害発生論理

この論理は、「１ブロック・シーケンス運転の完了以前」（Ed11,2）のために「動力源が存在する」（Ed11）論理以外はCase（a-1)と等価な論理となる。

手動停止機構のみを備えた系での災害発生論理を図６－５のＦＴとして示す。

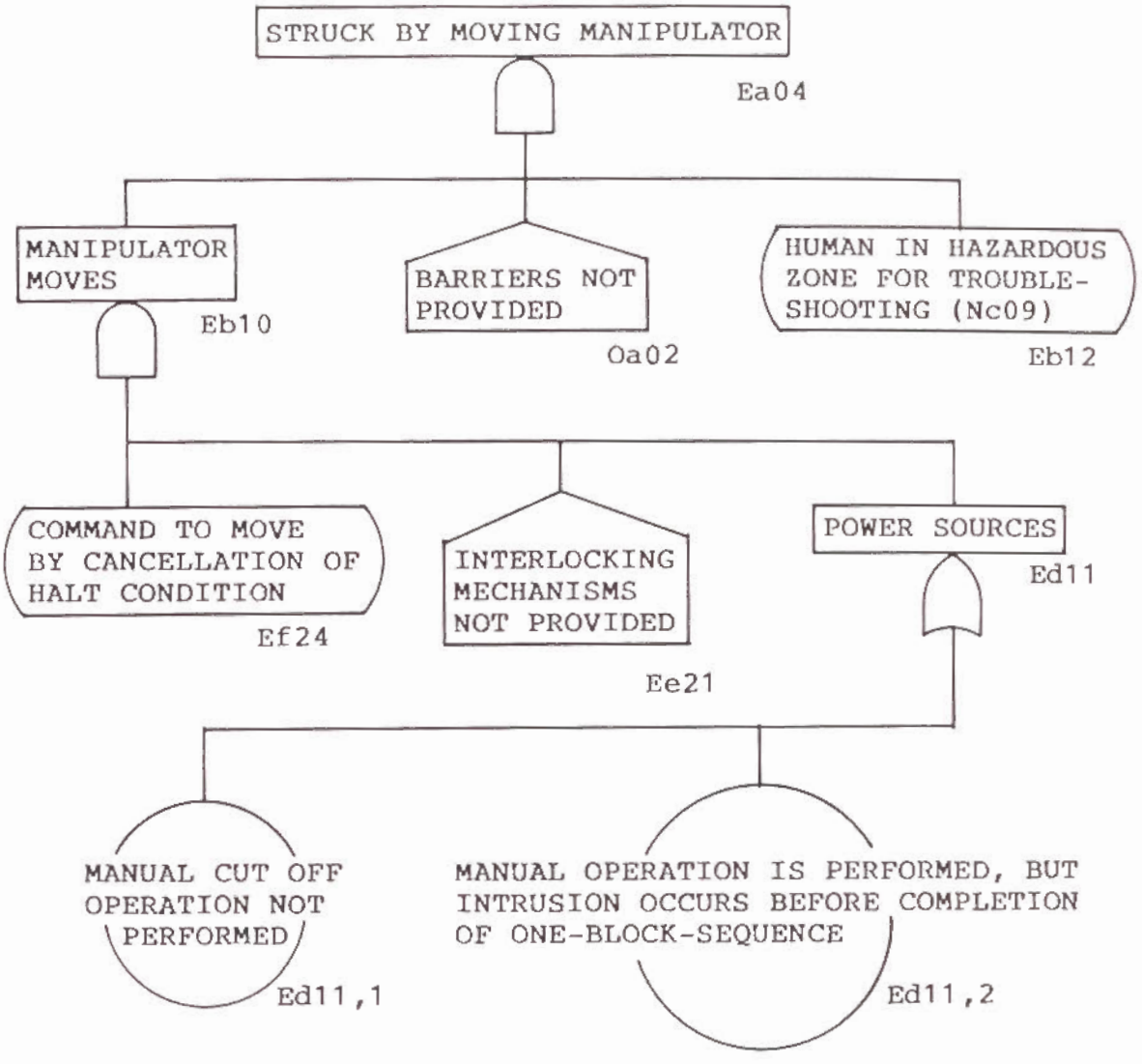


図６－５　特殊化されたＦＴ（手動停止機構を備えた系）

b．自動インターロッキング機構のみを備えた系

Case（b-1）：情報処理系の故障による災害発生論理

「情報処理系の故障」（Ed10,1）によるインターロッキングの失敗論理、および手動停止機構の「不設置」（Ed11,3）により動力源が常に存在する論理以外は、Case（a-1)と等価な論理となる。

Case（b-2）：動力源の故障による災害発生論理

「動力源の故障」（Ed10,2）によるインターロッキングの失敗論理以外は，Case（b-1)と等価な論理となる。

自動インターロッキング機構のみを備えた系での災害発生論理を図６－６のＦＴとして示す。

c．手動停止と自動インターロッキング機構を備えた系

Case（c-1）：停止操作の失敗と情報処理系の故障による災害発生論理

「停止のための操作を怠る」（Ed11.1'）による「動力源の存在」（Ed11'）論理以外は、Case（b-1)と等価な論理となる。

Case（c-2）：完全停止の確認失敗と情報処理系の故障による災害発生論理

「１ブロック・シーケンス運転の完了以前」（Ed11.2'）のために「動力源が存在する」（Ed11'）論理以外はCase（b-1)と等価な論理となる。

Case（c-3）：停止操作の失敗と動力源の故障による災害発生論理

「停止のための操作を怠る」（Ed11.1'）による「動力源の存在」（Ed11'）論理以外は、Case（b-2)と等価な論理となる。

Case（c-4）：完全停止の確認失敗と動力源の故障による災害発生論理

「１ブロック・シーケンス運転の完了以前」（Ed11,2'）のために「動力源が存在する」（Ed11'）論理以外はCase（b-2)と等価な論理となる。

手動停止と自動インターロッキングの両機構を備えた系での災害発生論理を図６－７のＦＴとして示す。

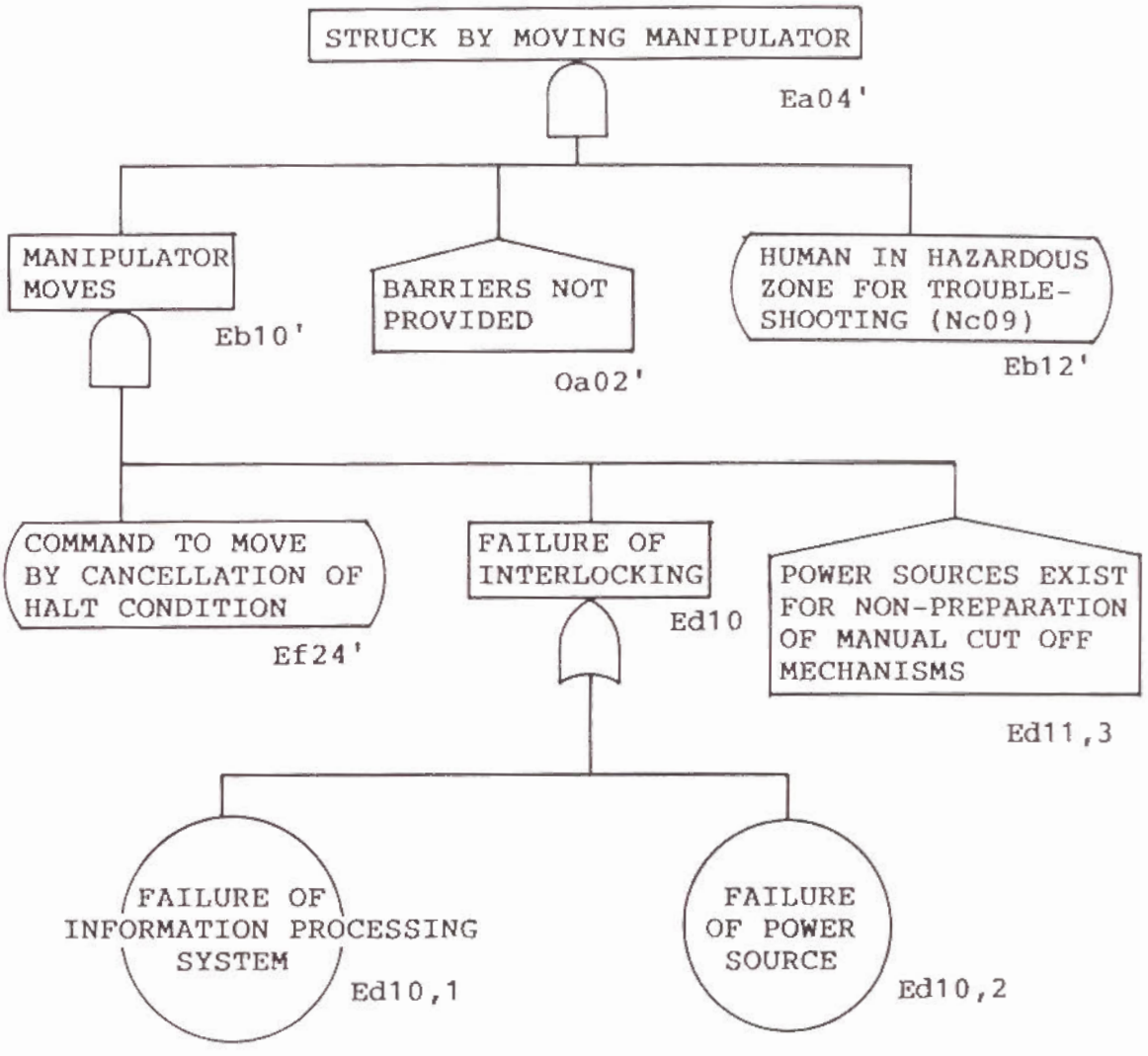


図６－６　特殊化されたＦＴ（自動インターロッキング機構を備えた系）

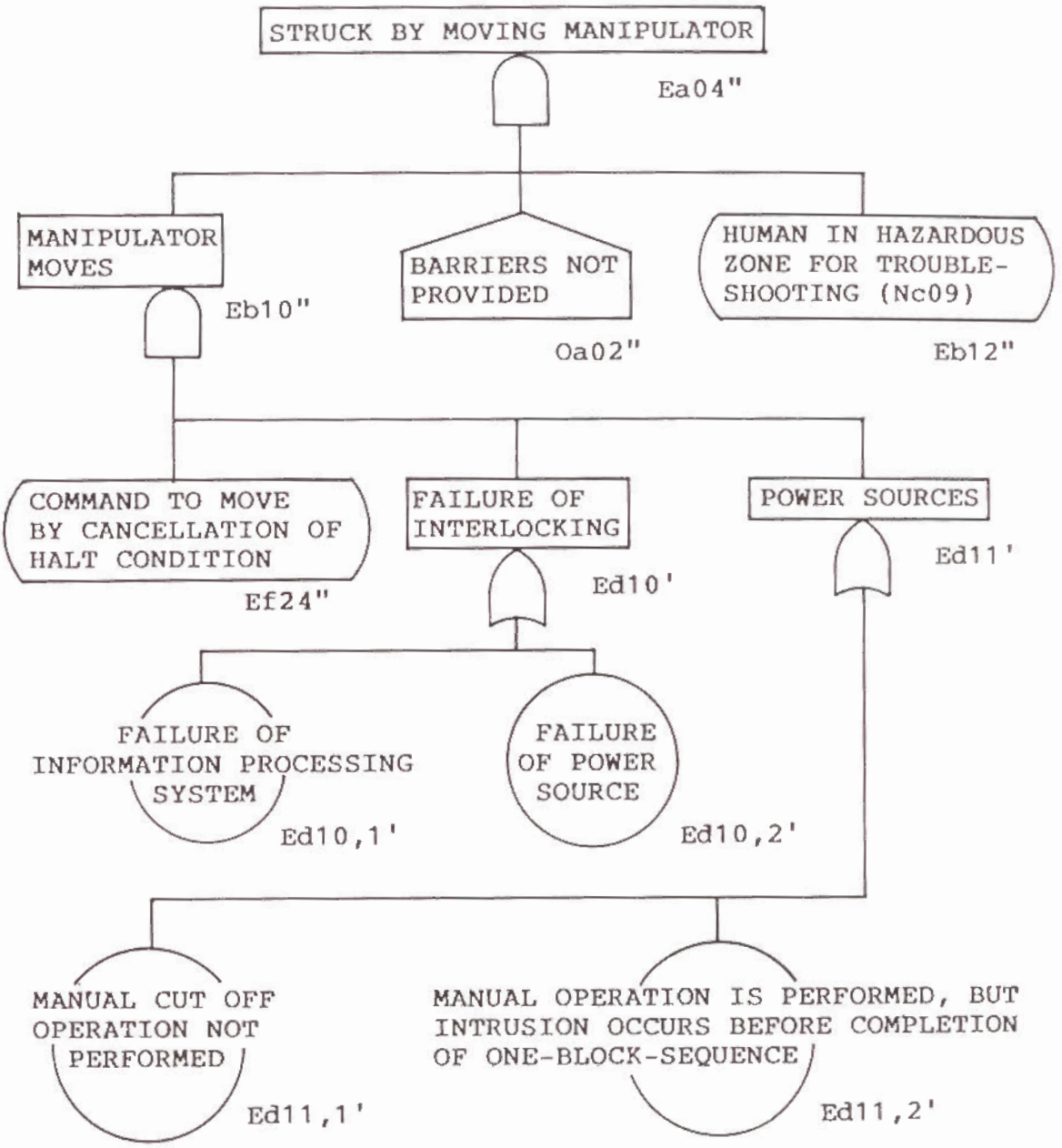


図６－７　特殊化されたＦＴ（手動停止機構と自動インターロッキング機構を備えた系）

6．5．3　各潜在危険制御系を備えた系における最小カット集合

各潜在危険制御系を備えた系のＦＴより、各系における最小カット集合が次のように得られる。

ａ．手動停止機構のみを備えた系

Case (a-1): $C(x)_{a1}$ = {Ef24, Ed11, 1, Nc09}　(6-7)

Case (a-2): $C(x)_{a2}$ = {Ef24, Ed11, 2, Nc09}　(6-8)

ｂ．自動インターロッキング機構のみを備えた系

Case (b-1): $C(x)_{b1}$ = {Ef24', Ed10, 1, Nc09'}　(6-9)

Case (b-2): $C(x)_{b2}$ = {Ef24', Ed10, 2, Nc09'}　(6-10)

ｃ．手動停止と自動インターロッキング機構を備えた系

Case (c-1): $C(x)_{c1}$ = {Ef24", Ed10, 1', Ed11, 1', Nc09"}　(6-11)

Case (c-2): $C(x)_{c2}$ = {Ef24", Ed10, 1', Ed11, 2', Nc09"}　(6-12)

Case (c-3): $C(x)_{c3}$ = {Ef24", Ed10, 2', Ed11, 1', Nc09"}　(6-13)

Case (c-4): $C(x)_{c4}$ = {Ef24", Ed10, 2', Ed11, 2', Nc09"}　(6-14)

6．5．4　基本事象の生起条件

カットを構成する基本事象に、次のような生起条件を設定しても不自然では

ない。

条件１：連続運転モードでは、作業開始後十分時間の経過した定常状態で、単位時間当たり平均a_1個のワークが加工される。すなわちマニプレータは、図６－１に示された③→②→④→①→②→③の動作を平均a_1［時間$^{-1}$］行い、この動作持続時間は平均b_1^{-1}［時間］である。

条件２：作業者に危険域内での異常処理作業を行わせようとする事象の期待発生回数は，作業が開始されて十分時間の経過した定常状態でa_2［時間$^{-1}$］、また危険域内へとどまる時間の期待値はb_2^{-1}［時間］である。

条件３：作業者が危険域に入ろうとする条件下で、停止操作を怠る確率は、q_1（一定）である。

条件４：自動停止機構における情報処理系のMTTF(Mean Time To Failure)はa_3^{-1}［時間］、MTTR(Mean Time To Repair)はb_3^{-1}［時間］である。

条件５：動力源が誤って電力を供給する故障はリレーのopen側故障、または機械的構造の破壊により生じ、その発生確率は１作動要求あたりp_1（一定）である。

条件６：インターロッキングによる停止は、センサによる検出と同時に行われ、いったん停止すると、作業者が金網外へ出て再起動操作を行わないかぎり停止状態を保つ。また、センサは必ず作業者が危険域に入る前に検出するものとし、検出してから作業者が危険域に入るまでの時間は十分小さく無視できる。

条件７：作業者が手動停止操作を行った条件下で、マニプレータの完全停止の確認を怠り危険域に入ろうとする確率はq_2（一定）である。また、操作してから侵入しようとする時間は無視できる。

条件８：作業者が、事象Ed11.1, Ed11.2, Ed10.1, Ed10.2, Ed11.1', または Ed11.2' の条件下で、危険域に入ろうとしたとき、マニプレータが待機中では必ず侵入し、目前を動作している最中での侵入はまれであり無視できる。また、入ろうとしてから侵入完了までの時間は無視できる。

6．5．5　発生順序を考慮した最小カット集合

事象U_1，U_2，・・・，U_7をそれぞれ次ぎのようにと定義する：

U_1 ≡ {事象Ed11,1の条件での事象Nc09の生起}

U_2 ≡ {Ed11,2の条件下でのNc09の生起}

U_3 ≡ {Ed10,2の条件下でのNc09' の生起}

U_4 ≡ {Ed11,1' の条件下でのNc09" の生起}

U_5 ≡ {Ed11,2' の条件下でのNc09" の生起}

U_6 ≡ {Ed11,1' およびEd10,2' の条件下でのNc09" の生起}

U_7 ≡ {Ed11,2' およびEd10,2' の条件下でのNc09" の生起}

すると、6.5.3 節で得られたカットは、次のように書きかえられる：

$C(x)_{a1}$ = {Ef24, U_1 }　(6-15)

$C(x)_{a2}$ = {Ef24, U_2 }　(6-16)

$C(x)_{b1}$ = {Ef24', Ed10,1, Nc09'}　(6-17)

$C(x)_{b2}$ = {U_3 , Ef24'}　(6-18)

$C(x)_{c1}$ = {Ef24", Ed10,1', U_4 }　(6-19)

$C(x)_{c2}$ = {Ef24", Ed10,1', U_5 }　(6-20)

$C(x)_{c3}$ = {U_6 , Ef24"}　(6-21)

$C(x)_{c4}$ = {U_7 , Ef24"}　(6-22)

これらのカットの生起には、前章で与えられた条件６、８より：

（ｉ）事象Ed10,1、Ed10,1’がそれぞれ、事象Nc09’、U_4、U_5に先立って生起している。

（ii）事象U_1、U_2、Nc09’、U_3、U_4、U_5、U_6、U_7が、それぞれ事象Ef24、Ef24’、Ef24”に先立って生起している。

ことが必要である。

以上の条件を考慮したカットの生起の正確な論理は、優先AND ゲートを用いて、図６－８のように表現される。

６．６　定量的安全性解析

６．６．１　基本事象の定量化

基本事象の定量化に際し、次の仮定を置く。

仮定１：条件１より、事象 Ef24 、Ef24’、Ef24” の生起は、定数発生率 a_1 b_1 ／（b_1 － a_1）［時間$^{-1}$］と修復率 b_1 ［時間$^{-1}$］の指数分布でモデル化される。

仮定２：条件２より、事象Nc09、Nc09’、Nc09” の生起は、定数発生率 a_2 b_2 ／（b_2 － a_2）［時間$^{-1}$］と修復率 b_2 ［時間$^{-1}$］の指数分布でモデル化される。

仮定３：条件４より、事象Ed10,1、Ed10,1’ の生起は、定数発生率 a_3 b_3 ／（b_3 － a_3）［時間$^{-1}$］と修復率 b_3 ［時間$^{-1}$］の指数分布でモデル化される。

仮定４：基本事象は、その生起に関して統計的に独立で、時刻０で、それぞれ非生起とする。

６．６．２　カット発生回数評価のアルゴリズム

Casc（a-1）：事象U_1の生起は、仮定２および条件３などより、定数発生率 q_1 a_2 b_2 ／（b_2 － q_1 a_2）［時間$^{-1}$］と修復率 b_2 ［時間$^{-1}$］の指数

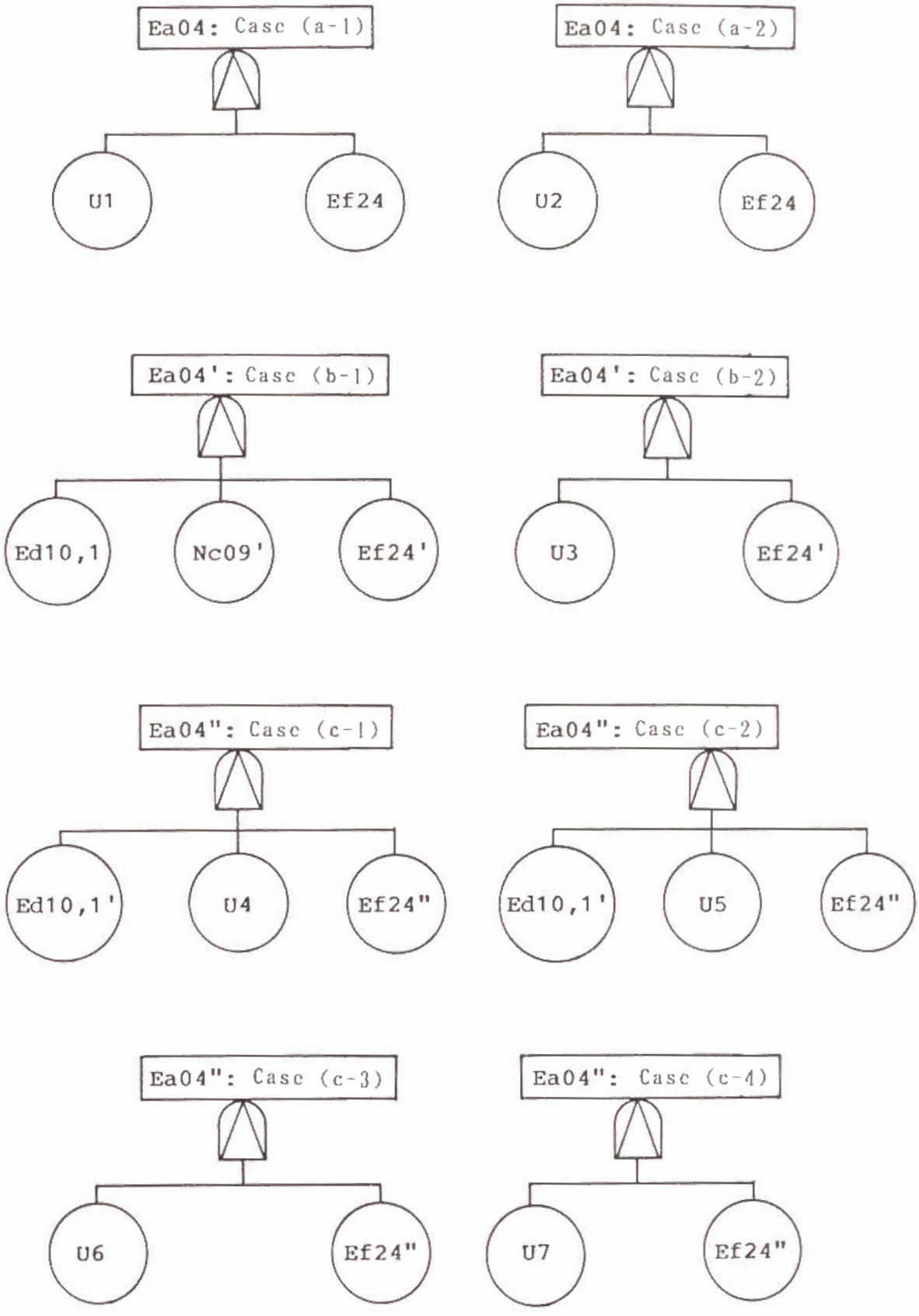


図６－８　基本事象の発生順序を考慮した最小カットＡＮＤ構造

分布に従う。さらに仮定（１）より、時刻零ですべての入力事象が非生起の条件下で、時刻ｔまでのこのカットの発生回数の期待値Ｗ＊(0,t) は、前章式(5-4)、(5-5)、(5-34)などから、２入力事象として得られる式(6-17)において、

$$\lambda_1 = q_1\ a_2\ b_2 \ /\ (b_2 - q_1\ a_2), \qquad \mu_1 = b_2$$

$$\lambda_2 = a_1\ b_1 \ /\ (b_1 - a_1), \qquad \mu_2 = b_1$$

として与えられる。

Case (a-2)：事象U_2の生起は、仮定２および条件６などより、定数発生率$(1-q_1)\ q_2\ a_2\ b_2 \ /\ \{b_2 - (1-q_1)\ q_2\ a_2\}$ [時間$^{-1}$] と修復率b_2 [時間$^{-1}$] の指数分布に従う。したがって、Case (a-1)と同様に、このカットの発生回数の期待値は、式(6-17)において、

$$\lambda_1 = (1-q_1)\ q_2\ a_2\ b_2 \ /\ \{b_2 - (1-q_1)\ q_2\ a_2\}, \qquad \mu_1 = b_2$$

$$\lambda_2 = a_1\ b_1 \ /\ (b_1 - a_1), \qquad \mu_2 = b_1$$

として得られる。

Case (b-1)：同様に、このカットの発生回数の期待値は、式(6-18)において、

$$\lambda_1 = a_3\ b_3 \ /\ (b_3 - a_3), \qquad \mu_1 = b_3$$

$$\lambda_2 = a_2\ b_2 \ /\ (b_2 - a_2), \qquad \mu_2 = b_2$$

$$\lambda_3 = a_1\ b_1 \ /\ (b_1 - a_1), \qquad \mu_3 = b_1$$

として与えられる。

Case（b-2）：同様に、このカットの発生回数の期待値は、式(6-17)において、

$$\lambda_1 = p_1 a_2 b_2 / (b_2 - p_1 a_2), \quad \mu_1 = b_2$$

$$\lambda_2 = a_1 b_1 / (b_1 - a_1), \quad \mu_2 = b_1$$

として与えられる。

Case（c-1）：同様に、このカットの発生回数の期待値は、式(6-18)において、

$$\lambda_1 = a_3 b_3 / (b_3 - a_3), \quad \mu_1 = b_3$$

$$\lambda_2 = q_1 a_2 b_2 / (b_2 - q_1 a_2), \quad \mu_2 = b_2$$

$$\lambda_3 = a_1 b_1 / (b_1 - a_1), \quad \mu_3 = b_1$$

として得られる。

Case（c-2）：同様に、このカットの発生回数の期待値は、式(6-18)において、

$$\lambda_1 = a_3 b_3 / (b_3 - a_3), \quad \mu_1 = b_3$$

$$\lambda_2 = (1 - q_1) q_2 a_2 b_2 / \{b_2 - (1 - q_1) q_2 a_2\}, \quad \mu_2 = b_2$$

$$\lambda_3 = a_1 b_1 / (b_1 - a_1), \quad \mu_3 = b_1$$

として得られる。

Case（c-3）：同様に、このカットの発生回数の期待値は、式(6-17)において、

$$\lambda_1 = q_1\ p_1\ a_2\ b_2 \,/\, (b_2 - q_1\ p_1\ a_2)\,, \qquad \mu_1 = b_2$$

$$\lambda_2 = a_1\ b_1 \,/\, (b_1 - a_1)\,, \qquad \mu_2 = b_1$$

として与えられる。

Case（c-4）：同様に、このカットの発生回数の期待値は、式(6-17)において、

$$\lambda_1 = (1 - q_1)\ q_2\ p_1\ a_2\ b_2 \,/\, \{b_2 - (1 - q_1)\ q_2\ p_1\ a_2\}$$

$$\mu_1 = b_2$$

$$\lambda_2 = a_1\ b_1 \,/\, (b_1 - a_1)\,, \qquad \mu_2 = b_1$$

として与えられる。

$$W^*(0,t) = \frac{\lambda_1}{\lambda_1+\mu_1}\ \frac{\lambda_2}{\lambda_2+\mu_2}\ \left[\mu_2 t - \frac{\lambda_2 \exp\{-(\lambda_2+\mu_2)\ t\}}{\lambda_2+\mu_2} + \frac{\mu_2 \exp\{-(\lambda_1+\mu_1)\ t\}}{\lambda_1+\mu_1} + \frac{\lambda_2 \exp\{-(\lambda_1+\mu_1+\lambda_2+\mu_2)\ t\}}{\lambda_1+\mu_1+\lambda_2+\mu_2} + \frac{\lambda_2}{\lambda_2+\mu_2} - \frac{\mu_2}{\lambda_1+\mu_1} - \frac{\lambda_2}{\lambda_1+\mu_1+\lambda_2+\mu_2}\right] \qquad (6-17)$$

$$W^*(0,t) = \prod_{i=1}^{3}\left(\frac{\lambda_i}{\lambda_i+\mu_i}\right)\ \left[\left\{\left(\frac{\mu_2}{\mu_1+\mu_2}\right) t + \frac{\mu_2 \exp(-(\lambda_1+\mu_1)\ t)}{(\mu_2-\lambda_1)\ (\lambda_1+\mu_1)} + \frac{\lambda_2 \exp(-(\lambda_2+\mu_2)\ t)}{(\lambda_2-\mu_1)\ (\lambda_2+\mu_2)}\right.\right.$$

$$\left.\left. - \left(\frac{\lambda_1}{\lambda_1+\lambda_2} + \frac{\mu_1}{\mu_1+\mu_2} + \frac{\mu_1}{\lambda_2-\mu_1} + \frac{\lambda_1}{\mu_2-\lambda_1}\right) \frac{\exp(-(\mu_1+\mu_2)\ t)}{\mu_1+\mu_2}\right.\right.$$

$$- \frac{\lambda_2 \exp(-(\lambda_1+\mu_1+\lambda_2+\mu_2)\ t)}{(\lambda_1+\lambda_2)\ (\lambda_1+\mu_1+\lambda_2+\mu_2)} \} \mu_3$$

$$+ \{ - \frac{\mu_2 \exp(-(\lambda_3+\mu_3)\ t)}{(\mu_1+\mu_2)\ (\lambda_3+\mu_3)} + \frac{\mu_2 \exp(-(\lambda_1+\mu_1+\lambda_3+\mu_3)\ t)}{(\mu_2-\lambda_1)\ (\lambda_1+\mu_1+\lambda_3+\mu_3)}$$

$$+ \frac{\lambda_2 \exp(-(\lambda_2+\mu_2+\lambda_3+\mu_3)\ t)}{(\lambda_2-\mu_1)\ (\lambda_2+\mu_2+\lambda_3+\mu_3)}$$

$$- \left(\frac{\lambda_1}{\lambda_1+\lambda_2} + \frac{\mu_1}{\mu_1+\mu_2} + \frac{\mu_1}{\lambda_2-\mu_1} + \frac{\lambda_1}{\mu_2-\lambda_1} \right)$$

$$\times \frac{\exp(-(\mu_1+\mu_2+\lambda_3+\mu_3)\ t)}{\mu_1+\mu_2+\lambda_3+\mu_3}$$

$$- \frac{\lambda_2 \exp(-(\lambda_1+\mu_1+\lambda_2+\mu_2+\lambda_3+\mu_3)\ t)}{(\lambda_1+\lambda_2)\ (\lambda_1+\mu_1+\lambda_2+\mu_2+\lambda_3+\mu_3)} \} \lambda_3$$

$$- \{ \frac{\mu_2}{(\mu_2-\lambda_1)\ (\lambda_1+\mu_2)} + \frac{\lambda_2}{(\lambda_2-\mu_1)\ (\lambda_2+\mu_2)}$$

$$- \left(\frac{\lambda_1}{\lambda_1+\lambda_2} + \frac{\mu_1}{\mu_1+\mu_2} + \frac{\mu_1}{\lambda_2-\mu_1} + \frac{\lambda_1}{\mu_2-\lambda_1} \right) \frac{1}{\mu_1+\mu_2}$$

$$- \frac{\lambda_2}{(\lambda_1+\lambda_2)\ (\lambda_1+\mu_1+\lambda_2+\mu_2)} \} \mu_3$$

$$- \{ - \frac{\mu_2}{(\mu_1+\mu_2)\ (\lambda_3+\mu_3)}$$

$$+ \frac{\mu_2}{(\mu_2-\lambda_1)\ (\lambda_1+\mu_1+\lambda_3+\mu_3)}$$

$$+ \frac{\lambda_2}{(\lambda_2-\mu_1)\ (\lambda_2+\mu_2+\lambda_3+\mu_3)}$$

$$- \left(\frac{\lambda_1}{\lambda_1+\lambda_2} + \frac{\mu_1}{\mu_1+\mu_2} + \frac{\mu_1}{\lambda_2-\mu_1} + \frac{\lambda_1}{\mu_2-\lambda_1} \right)$$

$$\times \frac{1}{\mu_1+\mu_2+\lambda_3+\mu_3}$$

$$- \frac{\lambda_2}{(\lambda_1+\lambda_2)\ (\lambda_1+\mu_1+\lambda_2+\mu_2+\lambda_3+\mu_3)} \} \lambda_3]$$

(6－18)

6．7　頂上事象の期待発生回数による安全性評価

本章で構成した潜在危険制御系を用いた系の安全性をＦＴの頂上事象の期待発生回数を求めることによって評価する。ここでは、系に以下の具体的な数値を設定する：

a_1（ワークの平均加工数）＝20［時間$^{-1}$］

b_1^{-1}（マニプレータの動作時間）＝9［秒］

a_2（異常処理作業期待発生回数）＝10^{-2}［時間$^{-1}$］

b_2^{-1}（危険域にとどまる平均時間）＝12［秒］

q_1（停止操作を怠る確率）＝q_2（完全停止の確認を怠る確率）

＝3×10^{-3}（怠りによる人的過誤確率[95]）

p_1（動力源の危険側故障発生確率）＝2×10^{-6}demand^{-1}（リレーのopen側故障確率[96]または機械的構造の破壊による失敗確率）

情報処理系のＭＴＴＦ（a_3^{-1}）＝ 3.33×10^3［時間］とし、

さらに情報処理系は、フェイル・セーフ度（F.S.D.）

$$F.S.D. \equiv （安全側故障率）／（危険側故障率） \qquad (6\text{-}19)$$

で定義されるF.S.D.が、それぞれ 0、10^2 、10^3 、10^4 、10^5 の各場合のものが利用できるものとする。また、このとき定期点検が無い場合における故障持続時間の期待値を（b_3^{-1}＝）50［時間］とし、危険側に故障中の情報処理系は定期点検によっても完全に新品のものと置き換えられるものとする。安全側に故障したときは、情報処理系はただちに新品のものと置き換えられるがこの影響はわずかであり無視する。

手動停止機構、自動インターロッキング機構、そして手動と自動の両機構を

備えた各系における頂上事象の10^4［時間］あたりの期待発生回数が図6－9のように得られる。

手動停止機構を備えた系の期待発生回数を基準にとれば、F.S.D.＝0の情報処理系を用いた自動インターロッキング機構を備えたの系では、点検間隔が50［時間］以上となると基準を満足しない。情報処理系のF.S.D.を高めるとそれに応じて系の安全性は向上するが、F.S.D.が10^5となったところで飽和し、これ以上F.S.D.を高めても安全性には変化が生じない。

これは、情報処理系のF.S.D.が高くなるに従って、相対的にそれ以外の故障モードの影響が支配的となるためである。

手動停止機構の場合では、本章のような系が10^4存在し、それらが10^4［時間］の連続自動運転を行うと、本章で特定した望ましくない頂上事象が400件近く発生することとなる。そして、そのうちの何割かは死亡や重傷災害につながることが考えられる。したがって、手動停止機構の場合には、必ずしも安全性が十分満足できるとは言いがたい。

本章のような条件にある人間－産業用ロボット系では、自動インターロッキング機構を備えることが望ましい。その際、F.S.D.を10^5まで高めることは非常に合理的である。

6.8 考 察

本章では、手動停止機構を備えた系の場合、10^4［時間］の連続自動運転として頂上事象の期待発生回数を求めている。現実には自動運転は種々の事情により中断される。しかし、式(6-17)からわかるように、事象の生起状態が速やかに定常状態となり、例えば、1［時間］以上連続自動運転モードが継続されると、非定常状態の影響はほとんど無視できる。したがって、連続の10^4［時間］は、各連続自動運転が1［時間］以上続くとき、それらの累積時間としてよい。

自動インターロッキング機構を備えた系の場合では、点検から次の点検まで

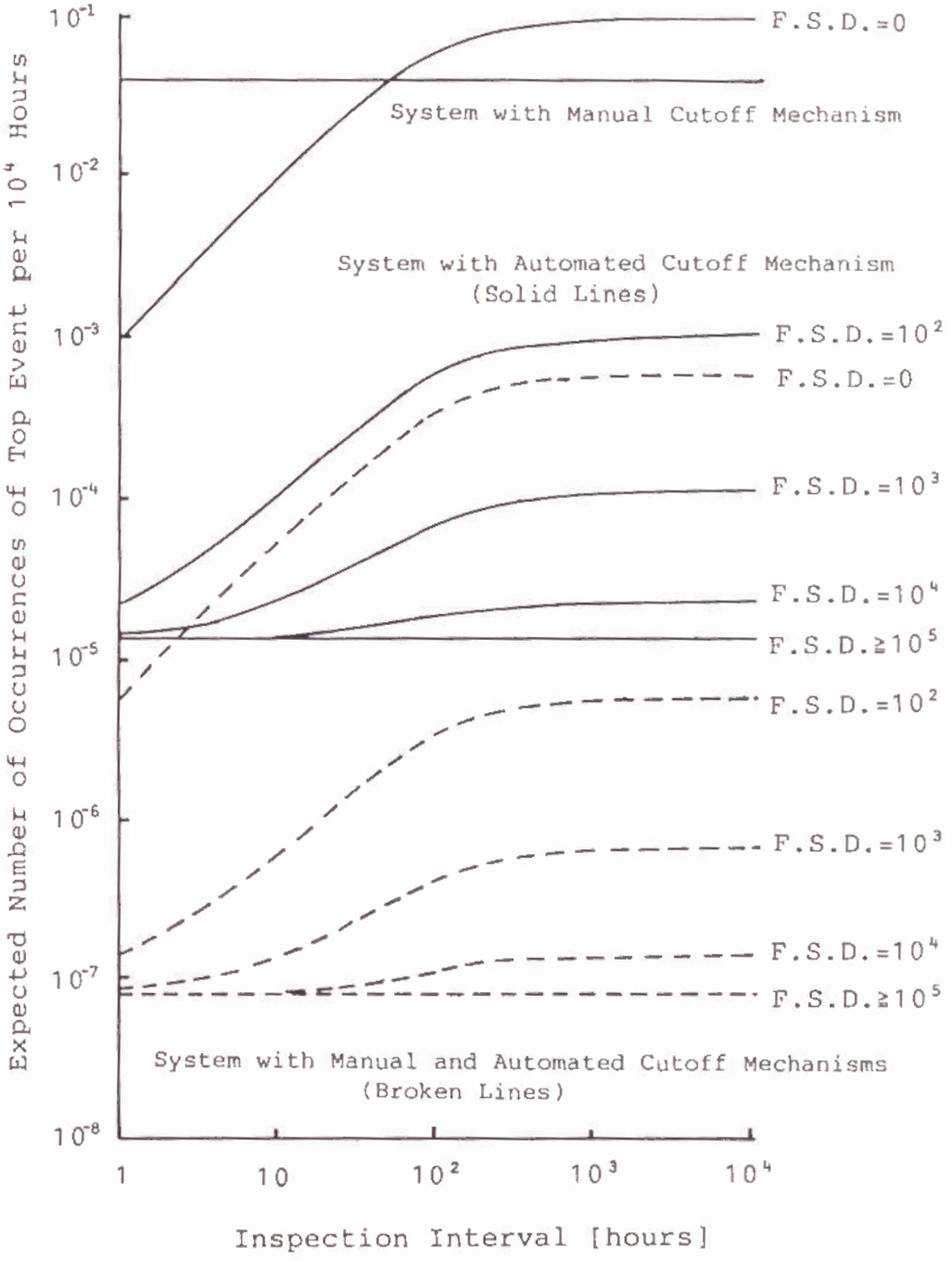


図６－９　１０⁴ 時間当たりの頂上事象期待発生頻度

の連続自動運転とし、その累積時間を10^4［時間］としている。この場合でも、1点検間隔内における中断回数がさほど多くなく中断時間もあまり長くないとき、発生回数を多少高く見積もることとなるが、本章での評価が許容されよう。中断時間が長い場合には、例えば、中断時間分の期待発生回数を差引くなどの処理が必要である。

本章では、作業者が危険域内に侵入するのはマニプレータが停止状態にあるときのみを考慮しているが、非常に稀であるがマニプレータが作動中にも危険域内に侵入することもあり得るであろう。これによる災害を防止するためには、図6－2の作用鎖［Ra ⟶₀］を解離する潜在危険制御系を構成しなければならない。これは、マニプレータの非常停止機構として概念化される。このような潜在危険制御系を構成した系の場合においても、本章で行ったものと同様にしてその安全性を解析・評価することができる。

6.9 結　言

本章では、これまでに論じてきた方法論を適用して、産業用ロボットを用いた無人加工セルの安全性を評価した。

まず、機械加工工場において典型的な、NCマシン、および加工物の自動供排給を行う産業用ロボットなどからなる無人加工セルを設定し、そこにおいて生ずる代表的な潜在危険をA－Cモデルにより同定した。

次に、同定された潜在危険に対して、潜在危険制御系をその構成法則に基づき系統的に構成した。それらは、ロボットの動力源を遮断する手動停止機構と自動インターロッキング機構として概念化される。

さらに、各機構を備えた系における災害発生論理が、災害発生機構の解析のための包括的論理モデルを系の条件に従って特殊化した個別的ＦＴとして展開され、基本事象の発生順序を考慮した最小カット構造が得られた。これらのカットを前章で述べたアルゴリズムを用いて定量化することにより、頂上事象の期待発生回数を求める方法を示した。

そして、系の各仕様条件に対し、その安全性を頂上事象の期待発生回数を求めることにより定量的に評価した。これに基づき、設定された系の仕様条件に関して、安全計画上求められる要件について論じた。

従来、安全性の事前評価は、航空・宇宙産業や原子力産業など新技術でかつ規模の大きい系を対象として実施されてきており、事前評価のための方法論もそれらの系を対象として研究・開発されてきた。本章で例示したように、新技術であるが比較的規模の小さく、しかし、人間やロボットの挙動の影響が大きいため複雑な災害発生論理となる「人間－ロボット系」においても、これまでに開発された方法論を適切に調整し、さらに本研究で展開された方法論を適用することによって、その事前安全性評価を行うことが十分可能である。

このような系統的な事前安全性評価の実施は、新技術を用いた系の安全性向上に欠くことのできない要件であると考えられる。

第７章　結　　論

本研究では、人間－ロボット系の安全性評価について論じた。

第１章では、これまで行なわれたロボットの安全性に関する研究の現状について概観し、人間－ロボット系の安全性評価の研究の必要性について言及した。すなわち、ロボットでは、従来の機械に比し、その安全化のための戦略が一層複雑となるため、系統的な安全計画を実施する必要がある。そして、安全計画全体の中での事前安全性評価の位置付けを明らかにし、その重要性を強調した。人間－ロボット系の安全性評価は、（１）潜在危険の同定、（２）潜在危険抑制措置の検討、（３）定性的安全性解析、（４）定量的安全性解析、の手順で行なわれる。

第２章では、人間－ロボット系の安全性評価の第１段階として、ロボットの人間に対する潜在危険を同定した。まず、毀損生成過程における系の要素間の関係を、作用－変化と作用連鎖モデルでモデル化・体系化した。これにより、潜在危険の概念およびその生成過程が明確化され、潜在危険が系統的に同定できるようになった。そして、作用－変化と作用連鎖モデルを用いて、ロボットにより生じ得る作用、作用連鎖そして各種要素の変化などが検討され、ロボットの人間に対する潜在危険が包括的に同定された。

第３章では、作用－変化と作用連鎖モデルを発展させることにより、潜在危険抑制措置の検討を系統的に行うための方法論を展開した。まず、潜在危険抑制過程を潜在危険抑制原理：（１）作用源の排除、（２）変化の抑制、（３）系の毀損生成相遷移の禁止、（４）系の毀損生成相からの遷移、として体系化し、従来使用されてきた各種安全技法がどの抑制原理に分類されるかを示した。次に、抑制原理（３）および（４）を実現する潜在危険抑制措置の構成法則を、

潜在危険制御系による作用鎖の解離法則として一般化・体系化した。この結果、複雑な系における潜在危険の同定過程と潜在危険制御系の構成過程とが有機的に関連付けられ、潜在危険制御系の構成を系統的に行うための方法論が確立された。これにより、フェイル・セーフなどの概念を明確化することにより、これまで異なる工学体系間に存在していた概念の不整合が解消され、フェイル・セーフの構成条件が明らかとなった。また、本方法論に基づき、自律移動ロボットの潜在危険抑制系が、ロボットの静止対象物との衝突潜在危険、および移動対象物のロボットとの衝突潜在危険に対して構成された。そして、潜在危険制御系の情報処理系が各潜在危険に対してどこまでフェイル・セーフ構成とされ得るかが明らかとなった。

第４章では、ロボットから人間への作用連鎖１形における運動エネルギ伝播作用により、人間がロボットの本体または腕によって打たれる災害発生の包括的論理モデルが、フォールト・ツリーの形式で展開された。このモデルにより、個々の具体的な系において実施されたそれらの災害に対する定性的安全性解析に見落しがないかをチェックすることができる。また、個々の系の災害発生論理として、この論理モデルを系の具体的諸条件に従って特殊化して与えることができる。さらに、系の定量的評価を行う際には、基本事象間に統計的独立性が仮定できることが重要であり、そのための手段として系の相分割を行うことの必要性を述べ相分割の方法を示した。そして、代表的な系の相における主要な最小カット集合を求め、それらカット集合を構成する各事象のフォールト・ツリー構成上の構造的な重要度を考慮することにより、系の各相において重要となる潜在危険抑制措置について論じた。

第５章では、安全性評価のために、これまでに原子力プラントなどを対象として開発されてきた定量的解析アルゴリズムが、人間－ロボット系の安全性評価にも適用できることを述べた。しかし、特に人間－ロボット系では、系の要素の故障発生順序が系の故障発生に本質的な影響を及ぼす、いわゆる順序依存

形故障論理が必要とされる場合が多いことを示し、順序依存形故障論理の定量化アルゴリズム開発の必要性を述べた。そして、フォールト・ツリーから得られる最小カット構造への入力事象が修復系で、それらが互いに統計的に独立であるとした条件下で、順序依存形故障論理の定量化アルゴリズムを提案した。このアルゴリズムにより、出力事象が時刻 t で生起している確率、出力事象の単位時間あたりの期待発生回数を簡便に求めることができるようになった。

第6章では、これまでに論じてきた一般化された方法論や包括的モデルを具体的な系に適用し、その安全性を評価した。まず、産業用ロボットを用いた無人加工セルを設定し、第2章で述べたモデルにより、そこで生ずる代表的な潜在危険を同定した。次に、第3章で展開された方法論に基づき、同定された潜在危険に対する潜在危険制御系を構成した。それらは、手動操作によりロボットの動力源を遮断する手動停止機構、および作業者の危険域内への侵入を検知して自動的にロボットの動力源を遮断する自動インターロッキング機構として概念化される。さらに、系の災害発生論理が、第4章で得られた包括的災害発生論理モデルを特殊化して、個別化されたフォールト・ツリーとして展開され、基本事象の発生順序を考慮した最小カット構造が得られた。これを前章で述べたアルゴリズムを用いて定量化することにより頂上事象の期待発生回数を求め、系の各場合における安全性を定量的に評価した。そして、設定された系における潜在危険抑制措置に求められる仕様条件が論じられた。

従来、安全性の事前評価は、航空・宇宙産業や原子力産業など規模の大きい系を対象として実施されてきており、その方法論もそれらの系を対象として研究・開発されてきた。人間－ロボット系など、規模はそれ程大きくないものの、柔軟で複雑な系に対しても、従来の方法論を適切に調整し、さらに本研究で展開した方法論を適用することによって、その事前安全性評価を実施することができる。系統的な事前安全性評価の実施は、新技術を用いた系の安全性向上に欠くことのできない要件である。

謝　　辞

本研究は、小職が労働省産業安全研究所、および京都大学精密工学教室にて文部省受託研究員、さらにテキサス州立ヒューストン大学にてパートキャランティ研究員として行った研究の成果を、京都大学航空工学教室・井上紘一教授の御指導のもとに纏めたものである。また、同大学工学部・吉川恒夫教授、同じく片山徹教授には、論文を纏めるにあたり貴重な御助言を賜りました。

ヒューストン大学・E．J．ヘンリー教授および京都大学精密工学教室・熊本博光助教授には、小職がそれぞれヒューストン大学および京都大学へ留学いたして以来今日まで御指導・御鞭撻をいただきました。

また、東京大学工学部・北森俊行教授、東京大学名誉教授・難波桂芳博士、埼玉工業大学名誉教授・井上威恭博士、東京都立科学技術大学・鈴木喜久教授、筑波大学電子・情報工学系・稲垣敏之助教授、京都大学航空工学教室・幸田武久博士、千代田工商（株）中村林二郎博士、横浜国立大学工学部・関根和喜助教授、（社）産業安全技術協会・近藤太二氏、同・川口邦供氏、東京大学工学部・広瀬通孝助教授、中央大学理工学部・塩見弘教授、（社）仮設工業会・森宜制博士、川崎重工業（株）大田芳晴氏、および（財）鉄道総合技術研究所・秋田雄志氏には、論文を纏めるにあたり有意義な御指摘と御討議をいただきました。

本研究の遂行に際して、なみなみならぬ御配慮と御助力を頂きました産業安全研究所機械研究部部長・橋内良雄博士、同じく前部長・加藤明氏、本研究に不可欠であった御助言と御鞭撻を頂きました先輩および同僚諸氏、さらに小職がこの方面の研究を行う機会を設けて下さいました産業安全研究所・元機械研究部長・近藤太二氏、産業安全研究所・元所長・秋山英司氏、同前所長・前郁夫氏、同現所長・田中隆二博士をはじめとして産業安全研究所および労働省安全衛生部の関係各位に衷心より御礼申し上げます。

参 考 文 献

1) H. Kumamoto, Y.Sato and K. Inoue : Engineering Risk and Hazard Assessment (Hazard identification and safety assessment of human-robot systems), CRC Press, Inc., Boca Roton, Florida,pp61-80,(1988).

2) B. C. Jiang and C. A. Gainer: A cause-and-effect analysis of robot accidents, Jour.of Occupational Accidents,Vol.9,NO.1,pp27-45,(1987).

3) 吉川：ロボットと人間，ＮＨＫブックス 475，ＮＨＫ出版協会、東京、(1985).

4) 加藤：からくりからマイロボットへ，機械学会誌、Vol87，No792，pp1241-1247，(1984)。

5) 労働省安全衛生部安全課：安衛則通覧（ロボット条項），労働基準調査会、東京、(1983).

6) ISO/TC184/SC2/WG3 ：Draft proposal of "manipulating idustrial robot-safety", ISO/TC/SC2, N166, pp1-27, (1988).

7) 佐藤、井上：ロボットの安全性について，機械学会誌、Vol90，No827，pp105-109，(1987).

8) 加藤、山下：人の特性・ロボットの特性（家庭生活アシストロボットを例として），ロボット学会誌、Vol4，No6，pp670-674，(1986).

9) J. M. Dolan, M. B. Friedman, M. L. Nagurka and J. K. Gotow: A robot in an operating room, Proc. Annu. Conf. IEEE Eng. Med. Biol. Soc., Vol9, No2, pp1096-1097, (1987).

10) 舟久保：医療とロボット，医科器械学、Vol54，No5，pp221-224，(1984).

11) 花安：建設工事労働災害の統計学的分析と安全性評価に関する研究，北海道大学学位論文、(1988).

12) U.S.AEC.: Reactor Safety Study (WASH-1400), (1974).

13) H.W.Heinrich, D.Petersen and N.Roos: Industrial Accident Prevention,

McGRAW HILL, BOOK CO., New York, p130, (1980).

14) H. Ozog: Hazard identification, analysis and control, Hazard Prevention, May/June, pp11-18, (1985).

15) 杉本：産業用ロボット，機械設計、Vol20, No1, pp56-61, (1976).

16) 土橋、荒谷：アーク溶接ロボットの機構と特性，機械設計、Vol20, No3, pp111-115, (1976).

17) H. J. Preis: Arbeitssicherheit beim Einsatz von Montage- und Handhabungsgeräten, VDI Ber, No323, pp183-188, (1978).

18) H. H. Muldau: Sicherheit am Arbeitsplatz Industrie-Roboter, Int. Conf. Ind. Robot Technol, Vol4, No1, pp24-34, (1978)

19) H. Inaba, S. Sakakibara: Unmanned machine tool system with an industrial robot, Int. Symp. Ind. Robots, Vol9, pp29-38, (1979).

20) J. Carlsson: Industrial robots and occupational accidents, Arbetsolycksfallsgruppen, Tekniska Högskolan, (1979).

21) P. Nicolaisen: Entwickeln problemangepasster Sicherheitseinrichtungen Beispiel Industrieroboter, Ind. Anz., Vol102, No73, pp64-65, (1980).

22) 川口、杉本、佐藤：産業用ロボットの危険性とFTA，RIIS-TN-82-1,(1982).

23) 川口、杉本：産業用ロボットの安全問題と対策，機械学会誌、Vol85,No766, pp1063-1068, (1982).

24) 佐久間：産業用ロボットの33の危険要因，IEレビュー、Vol23, No2, pp64-68, (1982).

25) R. D. Kilmer: Safety sensor systems for industrial robots, Tech. Pap. Soc. Manuf. Eng., No.MS-82-221, pp1-13, (1982).

26) Y. F. Yong, M. C. Bonney, N. K. Taylor: Safety and industrial robot systems (How CAD can help), IEE Conf. Publ.,No212, pp246-249,(1982).

27) K. G. Griffin: Safety for industrial robotic applications, Professional Safety, Vol28, No12, pp22-26, (1983).

28) M. A. Akeel: Intrinsic robot safety, Professional Safety, Vol28, No12, pp27-31, (1983).

29) J. H. Graham, J. F. Meagher, S. J. Derby: A safety and collision avoidance system for industrial robots, Conf. Rec. IEEE IAS Annu. Meet., Vol19, pp306-313, (1984).

30) 長町、穴山、伊藤、行待：産業用ロボットの人間工学的研究（ロボット操作における人間の信頼性について）、人間工学、Vol20, No1,pp55-63,(1984).

31) K.Khodabandchloo, F.Duggan, T.M.Husband: Reliability of industrial robot (A safety viewpoint), Proc. 7th Britsh Rob. Assoc. Annu. Conf. 1984, pp243-255, (1984).

32) M. Rahimi: System safety approach to robot safety, Proc. Hum.Factors Soc. Annu. Meet., Vol28th, No.vol.1, pp102-106, (1984).

33) L. H. J. Goossens: Risk assessment of robot systems, Paper presented at Symposium on Robot Safety, pp1-15, Delft, (1989).

34) R.Jones, S.Dawson: People and robots (their safety and reliability), Proc. 7th British Rob. Assoc. Annu. Conf.1984, pp243-255, (1984).

35) P. Nicolaisen: Überlegungen zur Arbeitssicherheit beim Einsatz von Industrierobotern, DVS Ber., Vol94, pp95-98, (1985).

36) D. W. Gage: Security considerations for autonomous robots, Proc. Symp. Secur. Privacy, Vol1985, pp224-228, (1985).

37) S.Derby, J.Meagher, J.Graham: A robot safety and collision avoidance controller, Tech. Pap. Soc. Manuf. Eng., No.MS-84-451,pp1-11,(1984).

38) C. A. Ramirez: Robotic intelligent safety system, Tec. Pap. Soc. Manuf. Eng., No.MS-84-434, pp1-13, (1984).

39) K. Kittiampon, J. E. Sneckenberger: A safety control system for a robotic workstation, Proc. Ann. Control Conf., Vol1985, No.Vol.3, pp1463-1465, (1985).

40) M. Harless, M. Donath: Tech. Pap. Soc. Manuf. Eng., No.MS-85-618,

pp1-13, (1985).

41) C. A. Ramirez: Artificial intelligence applied to robot fail-safe operations, Tech. Pap. Soc. Manuf. Eng., No.MS-85-619, pp1-18,(1985).

42) R. Joners, S. Dowson: The role of hardware, software and people in safeguarding robot production systems, Proc. 15th Int. Symp. Ind. Rob., Vol2, pp557-568, (1985).

43) J. H. Graham: An evidential approach to robot sensory fusion, IEEE Proc. Int. Conf. Cybern. Soc., Vol1986, No1, pp492-497, (1986).

44) T.J.Beugelsdijk, D.W.Knobeloch: Robots in radiation environments, J. Liq. Chromatogr., Vol9, No14, pp3093-3131, (1986).

45) M.Weck, H.Schönbohm: Sicherheitseinrichtungen für Industrieroboter-arbeitsplätze, VDI Z, Vol129, No3, pp63-67, (1987).

46) 藤井、岡：塗装用ロボットの安全性、機械学会誌、Vol90, No827, pp1356-1361, (1987).

47) D. L. Clem: Safety considerations for space robots, Rob.Expert Syst. 1986, pp.33-36, (1986).

48) 池田、野崎、島田、田島：壁面歩行ロボットに関する基礎的研究Ⅰ、機技研所報、Vol42, No3, pp117-128, (1988).

49) T. Marton, J. L. Pulaski: Assessment and development of HF related safety designs for industrial robots and robotic systems, Proc. Hum. Factors Soc. Annu. Meet., Vol31, No1, pp176-180, (1987).

50) 佐藤、井上：人間－ロボット系の安全性評価（作用－変化と作用連鎖モデルによる潜在危険の同定）、機械学会論文集（C編）、Vol51,No468, pp2188-2195, (1985).

51) Y. Sato, K. Inoue: Safety assessment of human-robot systems (Hazard identification based on the action-changes and action-chains models) Bull. JSME, Vol29, No250, pp1356-1361, (1986).

52) 佐藤、井上、熊本：人間－ロボット系の安全性評価（災害発生機構の解析の

ための論理モデル－その１）、機械学会論文集（Ｃ編）、Vol52, No474, pp823-832, (1986).

53) Y. Sato, K. Inoue, H. Kumamoto: The safety assessment of human-robot systems (Logic models for the analysis of the accident-causing mechanisms-Part 1), Bull. JSME, Vol29, No256, pp3618-3625, (1986).

54) 佐藤、井上、熊本：人間－ロボット系の安全性評価（順序依存形故障論理の定量化について）、機械学会論文集（Ｃ編）、Vol52, No475, pp1110-1117, (1986).

55) Y.Sato, K.Inoue, H.Kumamoto: The safety assessment of human-robot systems (On the quantification of consecutive failure logic), Bull. JSME, Vol29, No257, pp3945-3951, (1986).

56) 佐藤：新技術を用いたシステムに生ずる潜在危険の評価、RIIS-SRR-86.No1, pp103-117, (1986).

57) Y.Sato, H.Kumamoto, K.Inoue: On hazard identification and analysis of human-robot systems, Proc.Japan U.S.A. Symp. Flexible Automation, pp679-684, Osaka,(1986).

58) 佐藤、井上、熊本：人間－ロボット系の安全性評価（１台のハンドリング産業用ロボットの潜在危険抑制措置の評価）、機械学会論文集（Ｃ編）、Vol52, No482, pp2754-2763, (1986).

59) Y. Sato, K. Inoue, H. Kumamoto: The safety assessment of human-robot systems (Evaluation of hazard control measures for an industrial robot handling work pieces), JSME Intr. Jour., Vol30, No260, pp350-356, (1987).

60) Y. Sato, K. Inoue, E. J. Henley: Hazard assessment of industrial robots, Proc. U.S.A.-Japan Symp. Flexible Automation, Vol2, pp703-707, Minneapolis, (1988).

61) 佐藤、井上：人間－ロボット系の安全性評価（潜在危険制御系の構成原理）、機械学会論文集（Ｃ編）、Vol54, No505, pp2164-2173, (1988)

62) 佐藤、井上：ヒューマン・インターフェースにおける安全計画、第４回ＨＩＳ論文集、pp215-225, 東京、(1988).

63) Y.Sato, K.Inoue, E.J.Henley: The safety assessment of human-robot systems (Architectonic Principles of hazard-control systems), JSME Intr, Jour., Vol32, No1, pp67-74, (1989).

64) Y.Sato, E.J.Henley, K.Inoue: Architectonics of hazard-control systems for robotics, Proc. Intr, Conf. Advanced Mechatronics, pp415-420, Tokyo, (1989).

65) 佐藤、井上：人間－ロボット系の安全性評価（移動ロボットにおける潜在危険制御系の構成について）、機械学会論文集（Ｃ編）、Vol55, No.518, pp2663-2671, (1989).

66) 井上監修：ＦＴＡ安全工学、日刊工業新聞社、東京、(1979).

67) 文献 14).

68) 文献 66).

69) 文献 56).

70) W. G. Johnson: MORT Safety Assurance Systems, Marcel Dekker, INC., New York, p. 247, (1980).

71) 佐藤、杉本、前：マイクロエレクトロニクスを用いた自動生産システムの安全性評価（エネルギ転移連鎖と産業用ロボットの潜在危険）,RIIS-RR-32-5, pp1-10, (1984).

72) 榎本、佐々木：電気鉄道におけるフォールトトレランス技術、電学誌、Vol107、No4 、P.282, (1987).

73) E.J.Henley, H.Kumamoto: Designing for Reliability and Safety Control, Prentice-Hall Inc, Engle-wood Cliffs, N. J., (1985).

74) 奥村：コンピュータを用いたフェイル・セイフなシステム、情報処理、Vol22, No9、P.863, (1981).

75) 乾：カーエレクトロニクスと安全問題（現状および可能性）、電通学会報告、S-87-16, P.48, (1987).

76) 佐々木：鉄道における安全技術、電情通信学会報告、S87-13、P.30,(1987).

77) 文献 66).

78) 文献 70).

79) 文献 66).

80) R. Barlow, F. Proschan: Statistical Theory of Reliability and Life Testing, McArdle Press, Inc., Silver Spring, (1975).

81) E.W.Vesely, R.E.Narum: PREP and KITT; Computer cords for automatic evaluation of fault trees, IN-1349, (1970).

82) K. Inoue, E. J. Henley: Computer aided reliability and Safety analysis of complex systems, Proc. 6th IFAC Congr.,Vol26,No1,(1975).

83) J.B.Fussel, et al: On the quantitative analysis of priority AND failure logic, IEEE Trans. Reliab., Vol.R 25, No5, pp324-326,(1976).

84) H. Kumamoto, K. Tanaka, K. Inoue: Efficient evaluation of system reliability by Monte Carlo method, IEEE Trans. Reliab., Vol.R 26, pp311-315, (1977).

85) E.J.Henley, H.Kumamoto: Reliability Engineering and Risk Assessment, Prentice-Hall, Englewood Cliffs, New Jersey, (1981).

86) 文献 66)、82ページ.

87) 文献 83)、324 ページ

88) 佐藤：安全手段とコストの研究、第１５回安全工学研究発表予稿集、pp97-100, (1982).

89) N. R. Mann: Method for Statistical Analysis of Reliability and Life Data, John Willey & Sons, INC., New York, P.121, (1974).

90) 文献 83).

91) 文献 89).

92) Y. Sato, K. Inoue: On the quantification of consecutive failure logic, Procs. Intr. Symp. Reliability and Maintainability,(1990) Tokyo, pp552-557, (1990) June.

93) 文献 81).

94) 文献 1) の64ページ.

95) 文献 85)の286 ページ.

96) IEEE Std 500, Reliability Data, P.115, (1983).

97) Y.Sato, E.J.Henley, K.Inoue: An action-chain model for the design of hazard control systems for robots, IEEE Trans. Reliab.,Vol.39, No.2, pp151~157, (1990).

98) Y.Sato, E.J.Henley, K.Inoue: Structuring hazard-control systems for autonomous mobile robots, Proc. Japan U.S.A. Symp. Flexible Automation, Vol1, pp111~118, Kyoto,(1990) July.